Private Sector Bust: By - Shooting Shark :
The following article appeared in the August, 1985

On July 12, 1985, law enforcement officials seized the Private Sector BBS, the official computer bulletin board of 2600 magazine, for "complicity in computer theft," under the newly passed, and yet untested, New Jersey Statute 2C:20-25. Police had uncovered in April a credit carding ring operated around a Middlesex County electronic bulletin board, and from there investigated other North Jersey bulletin boards. Not understanding subject matter of the Private Sector BBS, police assumed that the sysop was involved in illegal activities. Six other computers were also seized in this investigation, including those of Store Manager [perhaps they mean Swap Shop Manager? - Shark] who ran a BBS of his own, Beowolf, Red Barchetta, the Vampire, NJ Hack Shack, sysop of the NJ Hack Shack BBS, and that of the sysop of the Treasure Chest BBS. Immediately after this action, members of 2600 contacted the media, who were completely unaware of any of the raids. They began to bombard the Middlesex County Prosecutor's Office with questions and a press conference was announced for July 16. The system operator of the Private Sector BBS attempted to attend along with reporters from 2600. They were effectively thrown off the premises. Threats were made to charge them with trespassing and other crimes. An officer who had at first received them civilly was threatened with the loss of his job if he didn't get them removed promptly. Then the car was chased out of the parking lot. Perhaps prosecutor Alan Rockoff was afraid that he presence of some technically literate reporters would ruin the effect of his press release on the public. As it happens, he didn't need our help. The next day the details of the press conference were reported to the public by the press. As Rockoff intended, paranoia about hackers ran rampant. Headlines got as ridiculous as hackers ordering tank parts by telephone from TRW and moving satellites with their home computers in order to make free phone calls. These and even more exotic stories were reported by otherwise respectable media sources. The news conference understandably made the front page of most of the major newspapers in the US, and was a major news item as far away as Australia and in the United Kingdom due to the sensationalism of the claims. We will try to explain why these claims may have been made in this issue. On July 18 the operator of The Private Sector was formally charged with "computer conspiracy" under the above law, and released in the custody of his parents. The next day the American Civil Liberties Union took over his defense. The ACLU commented that it would be very hard for Rockoff to prove a conspiracy just "because the same information, construed by the prosecutor to be illegal, appears on two bulletin boards." especially as Rockoff admitted that "he did not believe any of the defendants knew each other." The ACLU believes that the system operator's rights were violated, as he was assumed to be involved in an illegal activity just because of other people

under investigation who happened to have posted messages on his board. In another statement which seems to confirm Rockoff's belief in guilt by association, he announced the next day that "630 people were being investigated to determine if any used their computer equipment fraudulently." We believe this is only the user list of the NJ Hack Shack, so the actual list of those to be investigated may turn out to be almost 5 times that. The sheer overwhelming difficulty of this task may kill this investigation, especially as they find that many hackers simply leave false information. Computer hobbyists all across the country have already been called by the Bound Brook, New Jersey office of the FBI. They reported that the FBI agents used scare tactics in order

to force confessions or to provoke them into turning in others. We would like to remind those who get called that there is nothing inherently wrong or illegal in calling any ANY BBS, nor in talking about ANY activity. The FBI would not comment on the case as it is

an "ongoing investigation" and in the hands of the local prosecutor. They will soon find that many on the Private Sector BBS's user list are data processing managers, telecommunications security people, and others who are interested in the subject of the BBS, hardly the underground community of computer criminals depicted at the news conference. The Private Sector BBS was a completely open BBS, and police and security people were even invited on in order to participate. The BBS was far from the "elite" type of underground telecom boards that Rockoff attempted to portray. Within two days, Rockoff took back almost all of the statements he had made at the news conference, as AT&T and the DoD [Department of Defense - Shark] discounted the claims he had made. He was understandably unable to find real proof of Private Sector's alleged illegal activity, and was faced with having to return the computer equipment with nothing to show for his effort. Rockoff panicked, and on July 31, the system operator had a new charge against him, "wiring up his computer as a blue box." Apparently this was referring to his Novation Applecat modem which is capable of generating any hertz tone over the phone line. By this stretch of imagination an Applecat could produce a 2600 hertz tone as well as the MF which is necessary for "blue boxing." However, each and every other owner of an Applecat or any other modem that can generate its own tones therefore has also "wired up his computer as a blue box" by merely installing the modem. This charge is so ridiculous that Rockoff probably will never bother to press it. However, the wording of WIRING UP THE COMPUTER gives rockoff an excuse to continue to hold onto the computer longer in his futile search for illegal activity. "We have requested that the prosecutors give us more specific information," said Arthur Miller, the lawyer for The Private Sector. "The charges are so vague that we can't really present a case at this point." Miller will appear in court on August 16 to obtain this information. He is also issuing a demand for the return of the equipment and, if the prosecutors don't cooperate, will commence court proceedings against them. "They haven't been particularly cooperative," he said.

Rockoff probably will soon reconsider taking Private Sector's case to court, as he will have to admit he just didn't know what he was doing when he seized the BBS. The arrest warrant listed only "computer conspiracy" against Private Sector, which is much more difficult to prosecute than the multitude of charges against some of the other defendants, which include credit card fraud, toll fraud, the unauthorized entry into computers, and numerous others. Both Rockoff and the ACLU mentioned the Supreme Court in their press releases, but he will assuredly take one of his stronger cases to test the new New Jersey computer crime law. by seizing the BBS just because of supposed activities discussed on it, Rockoff raises constitutional questions. Darrell Paster, a lawyer who centers much of his work on computer crime, says the New Jersey case is "just another example of local law enforcement getting on the bandwagon of crime that has come into vogue to prosecute, and they have proceeded with very little technical understanding, and in the process they have abused many people's constitutional rights. What we have developing is a mini witch hunt which is analogous to some of the arrests at day care centers, where they sweep in and arrest everybody, ruin reputations, and then find that there is only one or two guilty parties." We feel that law enforcement, not understanding the information on the BBS, decided to strike first and ask questions later. 2600 magazine and the sysops of the Private Sector BBS stand fully behind the system operator. As soon as the equipment is returned, the BBS will go back up. We ask all our readers to do their utmost to support us in our efforts, and to educate as many of the public as possible that a hacker is not a computer criminal. We are all convinced of our sysop's innocence, and await Rockoff's dropping of the charges.

NOTE: Readers will notice that our reporting of the events are

quite different than those presented in the media and by the Middlesex County Prosecutor. We can only remind you that we are much closer to the events at hand than the media is, and that we are much more technologically literate than the Middlesex County Prosecutor's Office. The Middlesex County Prosecutor has already taken back many of his statements, after the contentions were disproven by AT&T and the DoD. One problem is that the media and the police tend to treat the seven cases as one case, thus the charges against and activities of some of the hackers has been

Phreaking AT&T Cards: By - Net Runner

My topic will deal with using an AT&T calling card for automated calls. Ok to place a call with an AT&T card, lift the handset (PAY PHONE) hit (0) and the desired area code and the number to call. Also when calling the same number that the card is being billed to you enter the phone number and at the tone only enter the last four digits on the card. But we don't want to do that now, do we. If additional calls are wanted all you do is hit the (#) and you will get a new dial tone! After you hit (#) you do not have to re-enter the calling card number simply enter your desired number and it will connect you. If the number you called is busy just keep hitting (#) and the number to be called until you connect! Ok to calL the U.S. of a from another country, you use the exact same format as described above! Ok now I will describe the procedure for placing calls to a foreign country, such as CANADA,RUSSIA,SOUTH AMERICA, etc.. Ok first lift the handset then enter (01) + the country code + the city code + the local telephone number. Ok after you get the tone enter the AT&T calling card number. Ok if you can not dial operator assisted calls from your area don't worry just jingle the operator and she will handle your call, don't worry she can't see you! The international number on the AT&T calling card is used for calling the US of A from places like RUSSIA, CHINA you never know when you might get stuck in a country like those and you have no money to make a call! The international operator will be able to tell you if they honor the AT&T calling card. Well I hope that this has straightened out some of your problems on the use of an AT&T calling card! All you have to remember is that weather you are placing the call or the operator, be careful and never use the calling card from your home phone!! That is a BIG NO NO.. Also AT&T has came out with a new thing called (NEW CARD CALLER SERVICE) they say that it was designed to meet the public's needs! These phones will be popping up in many place such as airport terminals, hotels, etc... What the new card caller service is, is a new type of phone that has a (CRT) screen that will talk to you in a language of your choice. The service works something like this, when you find a (NEW CARD CALLER PHONE), all you do is follow the instructions on the (CRT) screen, then you insert the (NEW CARD CALLER CARD) and there is a strip of magnetic tape on the card which reads the number, thus no one can hear you saying your number or if there were a bug in the phone,no touch tones will be heard!! You can also bill the call to a third party. that is one that I am not totally clear on yet! The phone is supposed to tell you how it can be done. That is after you have inserted your card and lifted the receiver!

♠

BASIC TELECOMMUNICATIONS: By - < Net Runner >

CN/A:

CN/A, WHICH STANDS FOR CUSTOMER NAME AND ADDRESS, ARE BUREAUS THAT EXIST SO THAT AUTHORIZED BELL EMPLOYEES CAN FIND OUT THE NAME AND ADDRESS OF ANY CUSTOMER IN THE BELL SYSTEM. ALL #'S ARE MAINTAINED ON FILE INCLUDING UNLISTED #'S.

HERE'S HOW IT WORKS:

1) YOU HAVE A # AND YOU WANT TO FIND OUT WHO OWNS IT, E.G. (914) 555-1234.

2) YOU LOOK UP THE CN/A # FOR THAT NPA IN THE LIST BELOW. IN THE EXAMPLE, THE NPA IS 914 AND THE CN/A# IS 518-471-8111.

3) YOU THEN CALL UP THE CN/A # (DURING BUSINESS HOURS) AND SAY SOMETHING LIKE, "HI, THIS IS JOHN JONES FROM THE RESIDENTIAL SERVICE CENTER IN MIAMI. CAN I HAVE THE CUSTOMER'S NAME AT 914-555-1234. THAT # IS 914-555-1234." MAKE UP YOUR OWN REAL SOUNDING NAME, THOUGH.

4) IF YOU SOUND NATURAL & CHEERY, THE OPERATOR WILL ASK NO QUESTIONS.

HERE'S THE LIST:

NPA	CN/A #	NPA	CN/A #
201	201-676-7070	517	313-232-8690
202	202-384-9620	518	518-471-8111
203	203-789-6800	519	416-487-3641
204	****N/A*****	601	601-961-0877
205	205-988-7000	602	303-232-2300
206	206-382-8000	603	617-787-2750
207	617-787-2750	604	604-432-2996
208	303-232-2300	605	402-345-0600
209	415-546-1341	606	502-583-2861
212	518-471-8111	607	518-471-8111
213	213-501-4144	608	414-424-5690
214	214-948-5731	609	201-676-7070
215	412-633-5600	612	402-345-0600
216	614-464-2345	613	416-487-3641
217	217-525-7000	614	614-464-2345
218	402-345-0600	615	615-373-5791
219	317-265-7027	616	313-223-8690
301	301-534-11??	617	617-787-2750
302	412-633-5600	618	217-525-7000
303	303-232-2300	701	402-345-0600

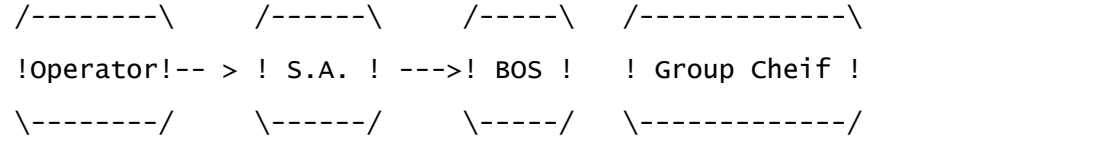
♠

304	304-344-8041	702	415-546-1341
305	912-784-9111	703	804-747-1411
306	****N/A*****	704	912-784-9111
307	303-232-2300	705	416-487-3641
308	402-345-0600	707	415-546-1341
309	217-525-7000	709	****N/A*****

312	312-769-9600	712	402-345-0600
313	313-223-8690	713	713-658-1793
314	314-436-3321	714	213-995-0221
315	518-471-8111	715	414-424-5690
316	816-275-2782	716	518-471-8111
317	317-265-7027	717	412-633-5600
318	318-227-1551	801	303-232-2300
319	402-345-0600	802	617-787-2750
401	617-787-2750	803	912-784-9111
402	402-345-0600	804	804-747-1411
403	403-425-2652	805	415-546-1341
404	912-784-9111	806	512-828-2502
405	405-236-6121	807	416-487-3641
406	303-232-2300	808	212-226-5487
408	415-546-1341		BERMUDA ONLY
412	412-633-5600	809	212-334-4336
413	617-787-2750	812	317-265-7027
414	414-424-5690	813	813-228-7871
415	415-546-1132	814	412-633-5600
416	416-487-3641	815	217-525-7000
417	314-436-3321	816	816-275-2782
418	514-861-6391	817	214-948-5731
419	614-464-2345	819	514-861-6391
501	405-236-6121	901	615-373-5791
502	502-583-2861	902	902-421-4110
503	503-241-3440	903	****N/A*****
504	504-245-5330	904	912-784-9111
505	303-232-2300	906	313-223-8690
506	506-657-3855	907	****N/A*****
507	402-345-0600	912	912-784-9111
509	206-382-8000	913	816-275-2782
512	512-828-2501	914	518-471-8111
513	614-464-2345	915	512-828-2501
514	514-861-6391	916	415-546-1341
515	402-345-0600	918	405-236-6121
516	518-471-8111	919	912-784-9111

A little something about Your phone company: By Col. Hogan

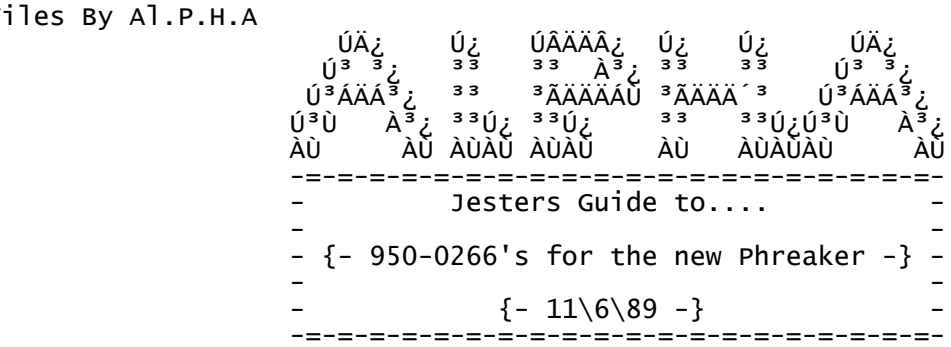
Ever get an operator who gave you a hard time, and you didn't know what to do? Well if the operator hears you use a little Bell jargon, she might wise up. Here is a little diagram (excuse the artwork) of the structure of operators



Now most of the operators are not bugged, so they can curse at you, if they do ask INSTANTLY for the "S.A." or the Service Assistant. The operator does not report to her (95% of them are hers) but they will solve most of your problems. She MUST give you her name as she connects & all of these calls are bugged. If the SA gives you a rough time get her BOS (Business Office Supervisor) on the line. S/He will almost always back her girls up, but sometimes

the SA will get tarred and feathered. The operator reports to the Group Chief, and S/He will solve 100% of your problems, but the chances of getting S/He on the line are nill. If a lineman (the guy who works out on the poles) or an Installation man gives you the works ask to speak to the Instal- lation Foreman, that works wonders. Here is some other bell Jar- gon, that might come in handy if you are having trouble with the line. Or they can be used to lie your way out of situations. An Erling is a line busy for 1 hour, used mostly in traffic studies A Permanent Signal is that terrible howling you get if you disc- connect, but don't hang up. Everyone knows what a busy signal is, but some idiots think that is the *Actual* ringing of the phone, when it just is a tone "beeps" when the phone is ringing, woul- ldn't bet on this though, it can (and does) get out of sync. When you get a busy signal that is 2 times as fast as the normal one, the person you are trying to reach isn't really on the phone, (he might be), it is actually the signal that a trunk line somewhere is busy and they haven't or can't reroute your call. Sometimes you will get a Recording, or if you get nothing at all (Left High & Dry in fone terms) all the recordings are being used and the system is really overused, will probably go down in a little while. This happened when Kennedy was shot, the system just couldn't handle the calls. By the way this is called the "reorder signal" and the trunk line is "blocked". One more thing, if an overseas call isn't completed and doesn't generate any money for AT&T, is is called an "Air & Water Call".

Files By Al.P.H.A



This is a file I just decided to write, right after a guy that lives near me, who runs a bbs complained about his outrageously high phone bill, and being that I use 0266's I decided that I would TRY to write a text file on how to use the 0266's as a simple way of phreaking. I am not an expert on the subject and I don't claim to be, I am just writing this file to try to help out others that are in the same experiance level as the guy that I was talking about previouly in the file.

There are many different types of 950's, but the type I use is the 950-0266 and I use these because that is what I was taught with and they seem like a fairly good, and easy way to phreak. 950-0266s are known to have VERY clean lines, so they are perfect to use with modems.

The basic format for these codes are:

(1) Dial 950-0266
(2) Wait for tone then dial your 7 digit Code
(3) Right after dialing your Code dial your ACN (Area Code Number)

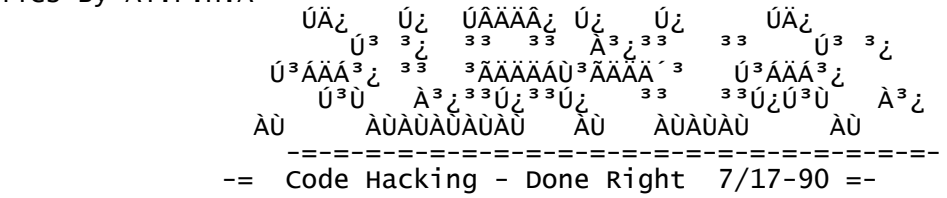
I.E. if I were to call my friend Joe in Utah, I would do this... 950-0266 (tone) XXXXXXX8015551234 The X's stand for the 7 digit code

950's have known to be dangerouse, they are on ESS (electronic switching service) which is a phreaks nightmare. Being that 950's are on the ESS they can, and have been known to trace. The type of tracing service on 950's can trace in a heart beat, so there is somewhat a great risk in using these. Some precautions about using 950s - Do NOT use the same code for more then 3 days. Try to use different codes if you have them i.e. call one board with a code like 2314211 , and then call the next board with a totally different code. Use these codes during prime time, to cut the risk of getting caught down. And use these in moderation, do not get crazy with them.

I hope this file hasnt been to much of a waste of time, I hope it has offered some help to you in using 950-0266's. I would like to have suggestions and comments on what you think of my file. If you have valid Input, please let me know your opinion on Al.P.H.A.'s home Board (801)!!!

Copyright (C) 1989 by -NecroiDaemon

Files By Al.P.H.A



-= Code Hacking - Done Right 7/17-90 =-

Code Hacking falls into both the hacking and phreaking category. Think about it. You have to HACK in order to get codez and then you PHREAK when you get the codez. I'm not going to go into great detail on code phreaking, this text file is going to deal mainly with "CODE HACKING". I get asked all the time where and how to get codez. I'm hoping this file will clear up this question for a lot of people. This is not my first text file, but I don't make a habbit out of them yet!

Code Hacking, What is it:
-=-=-=-=-=-=-=-=-=-=-=-=-

Simply enough it's where you get a dial up (IE. 1-800's or 950's) and set up a code hacking program and config it to the code you're about to hack and let it run. Now there are hundrends of dial ups for us pkreakers/hackers to play with (I will list a few at the end of this phile), and the code lenght and formats also very a great deal. Now you can get your hacker set up and let it run all night and if GhOd's willing you might get lucky and get a code by the next day.

Ok the best way to go about Code hacking is to get a format or template if you perfer to call it that. Now they look like this. 801XX, where you know the first 3 digits of the code is 801, but the last 2 digits are unknown and you have to hack out the last 2 digits. If you know all but 2 digits then you have a 1 in 100 shot in getting a code each time your hacker trys to hack a code, of course the longer the code or the less digits you know the less chance you have in hacking a code. But belive me it's never a lost cause. You can have zero digits and still get codez.

A Lesson in Formats #1:
-=-=-=-=-=-=-=-=-=-=-=-

Ok say your going to hack 1-800-635-9135, Code lenght is 5 digits, and already have the following codez!

22199
22723
22857
22832
21099

Ok, think about it for a second, we have 5 codez all staring with the # 2 and all but the last one has a 2 as the 2nd number, and the 3rd and 4th both have a 8 as the 3rd number and the 1st and 5th end with a 99, so you could user some different formats for this code and here the are:

22XXX
2XX99
228XX

Ok now there are a few formats for a 5 digit code. I think you can apply this same system to 6,7 or even 8 digit codez.

Well, I hope you can understand formats or templates a little better. Code hacking can be a long drug out process, but the way I look at it if you spend a night letting your hacker run and get a code and spend 5 hours or so of FREE ld calling then it's worth it.

A lesson in Formats #2:
-=-=-=-=-=-=-=-=-=-=-=-
Another probelem with code hacking is figure out or know what comes first the CODE or ACN (Area Code Number). On 950-0488's it's ACN + code, but on most 800's it's ACN + Code. There is really no way to know for sure. Just make sure when you get your starter codez (The ones you'll get your formats from) you know how to use them. If you know this it'll save you a lot of time. The Codes I gave above are CODE + ACN, but most 800's are ACN + Code. BTW as of the release date of this file the 800 number listed above works, but the codez are dead. Well thats the end of the FORMAT LESSONS.

What Code Hacker to Use:
-=-=-=-=-=-=-=-=-=-=-=-=
Well there are several hackers on the market, but your best bet is on one of two. Code Thief Deluxe by Phortune 500 and Brew Associates or Fucking Hacker by 2AF and Hypnacosm. I myself have played with both but Code Thief Deluxe v 4.0 is the best on the market. It's very user friendly and even the beginner can figure it out, but if you have a different hacker then fell free to use it. The Hacker you use should be the one you fell the best about. I like Theif 4.0 and I would recommend this to any and all hackers. The way I look at it, you can't go wrong with Phortune 500.

Dial up's and Code Lenths:
-=-=-=-=-=-=-=-=-=-=-=-=-=
1-800-222-4333 Code 6 Digits (Code + ACN)
1-800-657-9600 Code 7 Digits (Code + ACN)
1-800-327-9488 Code 13 Digits (Code + ACN)
1-800-476-4646 Code 6 Digits (Code + ACN)
1-800-234-5095 Code 6 Digits (Code + ACN)

950-0266 Code 7 Digits (ACN + Code)
950-0488 Code 13 Digits (ACN + Code)

Closing Notes.
-=-=-=-=-=-=-=
Well I hope the first text file from Al.P.H.A helps a few of you out. I was sitting arond (at work of all places) when it dawned on me I have never seen a file on code hacking, so I decided to do one up. This file is for the beginner not the Expert, but I have read a number of text files for beginners and have learned something from them. So enjoy.

Speical Thanks go out to:
-=-=-=-=-=-=-=-=-=-=-=-=-
Doc Silicon - (My Partiner in Crime) for talking me into starting this Awesome H&P group.

The Oxidizer - If it wasn't for your board, I'd of had to spent a lot more time Code Hacking.

|Brew Associates | - For the Awesome programming work that went into Theif
|<<<< P500 >>>>> | 3.5 and 4.0.
|Professor Falken| - For the Awesome work you did on your Phreak Tools

A Little About Al.P.H.A!
-=-=-=-=-=-=-=-=-=-=-=-=

We are a small group that plans on Hacking/Passing and Using codez. We started Al.P.H.A because we were tired of all the want-a-be groups we were a part of. I'm not going to state names of the Groups, I don't want a fucking war with any of them.

Al.P.H.A is:
-=-=-=-=-=

Captain Kidd - Doc Silicon - Techno Cyberdaeemon - Black Beard
Cristifer Columbus - Jester - Falcon

Files By Al.P.H.A

Surviving at Night: By Falcon

I am writing this file with the knowledge that night survival is a lot of common sense. I do however feel I can share some added information that can help make the anarchists favorite time of the day (night) a little safer and easier to work with. **note some of the information I am writing I have taken from a article from Combat Tactics magazine were as the rest is common sense and stuff I've picked up though personal night missions.

The first part of surviving at night is to dress accordingly. Common sense tell us a person in black clothing with a black mask is harder to spot then a person in white clothing. This of course is true, but one must also consider the fact that black is a stereotype for burglars, the devil and trouble its self. Not to mention a mask or painted face. That is why for most situations I recommend wearing modern, casual clothing that does not even need to be black. Dark blue or green etc. can accomplish the same over all effect at night. For summer try and have shorts, and dress accordingly to the season. Were black or dark socks and shoes. If you are running white shoes REALLY stand out. Also as I said before try to get around wearing a mask or face paint until the last minute possible.

You then need your equipment. I personally have a nice black pouch and belt I got from army navy surplus stores. I use the belt and pouch to hold all of my equipment, so if I have to I can drop the belt in a shadow, and look like a causal modern dressed dude walking to a friends house. We are talking innocent!!! In my ouch and belt I include: wire cutters, gloves black of, course to hide my little white hands and their fingerprints. A mask so I can hide my identity, a flashlight for seeing and destroying people's night vision- be careful not to shine it around windows etc. The same goes for matches, lighters because at night it is very obvious. A few bombs (CO2 etc.) to act as diversions and blow up stuff like mailboxes... A scope off a rifle. You would be surprise at how well you can see using on of them in the night, especially if you are looking toward light and your night vision is good. I do not recommend binoculars due to they take up both eyes and if you look into light you loose both eyes night vision.....

Also I take what ever else The situation requires. I try to not over-do-it. For example if you are only going on a scouting mission why danger yourself with a full load up. It is just more trouble you can get in, if caught. But also don't be under equipped or you could miss out on some killer opportunities. A favorite saying of mine (a quote from my hero the legendary assassin Jason Bourne: "opportunities will present themselves. When they do you better be ready to use them."

Night vision is important. To explain how it works one can compare the eye to a camera. The lens of an eye is like the lens of a camera focusing light as it enters. The iris of an eye is like the diaphragm of a camera opening and closing to allow the correct amount of light in for the situation. The retina is like film, light image is recorded and sent to the brain as light images thus producing pictures. We use two kinds of cells in seeing: Cone and Rod cells. (named due to their size).

Day vision comes from the cone cells. They enable you to see color, sharp contrast, and shape. The cone cells cannot function in low light levels, thus why we cannot see color at night.

The rod cells produce a substance called visual purple. This substance allows us to see at night. If we stare at something to long (a few seconds) all the visual purple in that spot of the eye is used up. This cause blank outs in what we're are starting at. To get around this problem scanning is used. Scanning is basically moving ones eyes back and forth never focusing on one spot. This allows the visual purple to evenly resupply itself so no black outs occur. When scanning never move your head back and forth (I will explain later) just your eyes.

The reason you should not move your whole head while scanning is because the human eye is very good at detecting movement. If you are being followed from a distance, or someone is looking for you just freeze. If you can lay prone, or get in a nice shadow, but in most situations you can be lost by anyone trying to find you. However if they have already located you, or they are very close you need to get away from them, then hide. If you are dressed correctly and freeze you can really be hard to spot. Also keep scanning so you don't get surprised by someone. If you must move do it slowly (including your head to scan behind you).

A very important fact in night vision is letting your eyes adjust to the dark. 30 minutes in the dark are required to completely adjust and get the best night vision. (you can spend 20 of the 30 minutes in red light and get the same effect, this can save time but who has a red lighted room?) Be careful with your night vision. It can be lost by looking into lights, a fire, etc. If you must go into light or look into it using a scope only use one eye. Cover the other eye so you at least have one good night eye at all times.

Practice these night sight tactics and become confident with the night. It is your friend!!

At night, our sound and movement become more trustworthy. That is why it is important to stay silent and well hidden. If you must talk do it in whispers and try to have a sign language

you can use to keep from having to talk. Certain areas are very dangerous at night. Areas like fences, rivers, roads, yards with dogs, open areas etc. If you must cross them make sure to stake

the area out so you know it is secure, then cross the danger area as fast as you can (don't become reckless but go fast.) Certain danger areas like dogs can be fixed. For example you could kill the dogs if give them meat to keep quiet.

Weapons of the night should try and be silent so they don't give away your position. Darts, air-guns, knives, silenced weapons etc. are best. However noise can be a great diversion. A timed fuse on a bomb can be used to attract attention to the wrong place allowing you to escape. Also say you are in a house and the owners come home and you are trapped in a room. Without killing them to get away unidentified you could beat them up with a mask on, but what if they were bigger then you? That's when a flashlight burst in a un-expecting face followed by a slam with your shoulders and your quick escape come in handy. Also you could buy a tear gas gun. I got mine for like 10-15 bucks and they are handy! You could pop some poor sucker in the face from a few feet away, slam him then run. The poor dude would be wondering if he had died and gone to hell as you ran for a safe place.

An important thing at night is to know your territory. Know were you can run and hide or get away. If you are in a new place scout it out. Also be good about keeping plans and sticking to them. Work in the buddy system so you aren't responsible for looking everyplace, and lugging all the supplies etc.

Well That is all I can think of at the time, I'm sure to remember more later.... I hope this file helps.....

Files By Al.P.H.A

BASIC CARDING (BY Al.P.H.A)

I would like to emphasize two facts:

Fact Number 1] Carding is dangerous, by reading this file, you are subjecting yourself to highly illegal information

Fact Number 2] Due to the fact of the illegality, I take NO responsibility for what actions might take place due to this file.

(Phew! now that that's over with...)

In this file we will discuss:

Chapter --> 1 Obtaining Cards

There are MANY ways to obtain cards, through Trashing (the art of scrounging through Garbage cans, and dumpsters and any other places that would be a good source of cut cards or carbons from receipts.) But that will be discussed in Trashing files available anywhere on your Average Phreak/Hack/Anarchy BBS/AE. You may also obtain them off a bbs with a Carding section, but to ensure best validity, get them yourself, as the motto goes,"If you want it done right the first time, do it yourself."

Chapter --> 2 Identifying/Checking the card

Checking the card is very simple, and even the novice carder can do it the first time. First, there are two ways (As far as i'm concerned) to check the card.

1] Using Tymnet, call your local dialup, and enter "TSDCOMPSUPP" for login. Then for the password, "HARRYHINES" will get you in. After your in, hit "?" for help, most likely you'll be using the option "B", remember using UPPERCASE. Where "B" is Mastercard / Visa transaction, but if you stumble across a Carta Blanche card, call me (Just kidding), then enter the letter for the transaction and you're off. It'll ask you for your card number, w/o the hyphens, then the experiation date, and amount you want to check the card for, a reasonable amount is 500.00, but you can experiment once you get more acquainted w/ it.

2] Using a computer voice driven checker, pevhaps a little faster, but a little more tricky. In order to use it, you must do the following:

Dial up the 800 watts, which is 1-800-554-2265, after you dial

it, it should ring and pick up, then a computer voice will say "Enter type" and then you respond with either:

10 for Mastercard
20 for Visa
Followed by a number sign will then ask for identification, hit "1067" preceeded by a number sign (always follow an entry w/ a number sign). It will say some bullshit and then ask you for your Merchant number in which you type 24 or 52 (whatever makes you happy) and then enter the card, after done it will ask for exp. date , then amount. Now, this is the tricky part, cuz if you fuck up here, it's gonna Decline you and you have to start ALL over. If your code is infact Valid, it will be followed by a Please Wait for 30-60 seconds and a Approved and a long number, don't worry about writing it down, just make sure to keep what you card to the limit the card can hold, or some calls might be made.

Chapter --> 3 Using the card for purchasing

You might think everything is pretty much a snap from here, but really this is where it gets difficult. Always order from a Mail-Order warehouse (OF course) If you're going to order from a Watts line, make sure you go through adleast Blue Boxing or Diverters before connecting w/ the company, for protection on Watts tracing.

After that, you must select an address (preferrably empty or abandoned) to ship the cargo to. And A) you also must make an awesomely authentic note with the card bearer's name on it saying you are out of town, and to leave it on the doorstep or B) be bold and face the UPS man and sign for it, but I suggest the note would be safer in more than one way. Then, order the merchandise, and if you don't sound old enough, get a friend or whoever to do the

talking. Another warning is that evidence has proved that purchasing relatively small priced items takes alot of worry from the company, thus, not resorting to do various checks on the card and the bearer's address.

Chapter --> 4 After the order, then what...

Well, after the package has arrived, casually pick it up (preferrably at night) and brisk it to your house. After that, I recommend that you don't just "HAPPEN" to pass by the house and stare it, that attracts attention, and believe me, that's the least thing you want. Try and stay far from the location, and NEVER use the same house twice.

I hope this file has helped you understand the BASIC principles of Carding, there is a lot more to learn, and there are a LOT more files like this to learn from. Stay cool... Take NOTE: The Watts dialups for the Credit Card verification # are in effect as

of this date, disonnections or changes in numbers I will try to handle. Same goes for the Tymnet verification ID & PASSWORD.

Carding:
~~~~~~~~~~

This is one that you can get in some major shit over. Well, although it is a major crime, it is really cool!!!! This is the process in which you find the card number of someone and use it to purchase things. In order to card, there are a few things that you must have or it will not work. You will need to have.....

1. The Card Number
2. The Experation date
3. Card type (Master Card, Visa, etc...)

Those are main things tha you will need. Having the name of the owner is very helpfull but it is not a must. You can get by without it. You have to order everything you want by mail. A couple of "Beginner" carder that I talked to didn't understand how you would do it, but thats when they had the misconception that you actually go to the store and purchase things. That is a complete No, no. You do everything from a phone ordering service. When you call make sure that you are at a pay phone. Don't do it your house or anywhere where it can come back to you. When you order the merchandice, once again do send it to anywhere that it can come back to you like your home, work, etc. Find a vacant house or building or anywhere else that you can send it to. Also, don't send it to a P.O. box that you have, just as dangerous. When you do order it and you think its around the time that you will be reciving it, check the mailbox frequently. But do it during odd hours. I mean, hows it going to look you taking a package from a vacant house?

Most bills are sent at the end of the month or at the biginning, so try to time it to where the bill won't come to the person untill a couple of days after you have recived the package. Ok heres how to figure it. I have found out that the bills are sent out up around the 26-30th of the month, so they will actually recive the bill around the 31-4th. Have it sent right after you think the bill has been sent. Find what you want, but try to order it from the place that guarentees the fastest delivery. When you order the item, make sure they have it in stock and don't have to get the item in first. Order the highest class of delivery but not COD or next day service. Thats cutting it too close. It should take around 2-4 weeks before you get it and if you timed it right, then it sound get there right before the person gets the bill. You need to have
~~~~~~~~~~

it in your possesion before the bill gets to the person because if they complain, they can keep it from being sent, or watch who actually gets it even while its going throught the mail process. Don't order more than a couple of things or overcharge the card,

if the people at the Credit card office, see irregular charging on the card, they will follow up on it.

To actually order the item you will call up the place that you will be ordering from, and when the operator answers let her know what you need to as far as what you are purchasing, etc. When she ask how you will be paying just tell her "Charge" and the the type of card like Master Card, Visa, ect. Then Tell them your name, if you don't know the name of the actuall owner of the card, Make up a false name that has NO relation to your name, not the same first, last middle what ever, nothing relating to your real name. Then continue answering all the operators questions, address (Not your own remember!) state, area code etc. They will also ask for your phone number. Make one up, not your own. If something happens to go wrong as far as delivery or if they are checking if you are who you say, then your screwed, unless of course, hehehe, the number is ALWAYS busy. Find the busiest number there is and leave them that. When they ask for the card number and experation, just tell them and do what all else you need. Wish them a good day, and hope you get it.

Ok heres how you check if the card is good, and how much money can be charged on the card..... 1. Dail 1-800-554-2265 2. it will ask for the type of the card. you must put in 10 for Master Card and 20 for Visa, I am not sure about the others. 3. Next it will ask for the Identification. You will need to enter 1067 4. After all that you will have to enter the Mecrchant number, which you will either need to put in 24 or 52. One of them should work. 5. You will then have to enter (When Prompted) the card number itself. 6. Next, the experation date of the card. 7. Last but not least the amount you want to try to get on the card. The procedure for this is enter dollars, astricks, then cents.

(Example:)
100*30 = One hundred dollars and thirty cents.

One thing I do need to mention, after you type in everything you must press pound (#). Like when it asks you for the type of card, if you had a Master Card you would put: 10#. when it asked for identification you would enter 1067#. If it says invalid, that either means that the card is no good or you can't charge that amount on the card. Try it again, but try a lower amount. If you get down to $1 and it still doesn't work, hehehe,
you can probably guess that the card is no good.

You might not be ordering just merchandice you might be ordering accounts and things like that and if you are, fine, but you have to remember, the accounts do not stay good for very long, the owner of the card gets the bill, complains and its no longer any good. And when you card and account, Nine out of ten times, they won't kill the account, they will trace in and that is when

you butts really in a sling. So carding accounts and hins, isn't the safest way to go, of course. nothing we have alked about it, right?

Introduction

carding is, in layman's terms, the use of someone elses credit card umber to obtain free merchandise. It can be used for things that re valuable to the BBS world like a USRobotics HST modem, or a rand new SCSI hard drive. The reason I am writing this article is because I, and the other notorious members of P/HARM have a multitude of wealth that some may deem useful. When I was a wee little mite, there was nothing to help me on my way..... So here goes....

Obtaining #s

There are many ways to obtain a credit card number. But the thing to remember is that there are three essentials that you need in order to use your number. 1) The name as it appears on the card, 2) The Card number, and 3) The actual date of expiration. These three things are not only essential, but if you get one of them wrong, it could send the FEDS huntin'. Okay, with that out of the way, now comes places to find the numbers. My most favorite, but the most time tested method is Trash bin hunting.... Nowadays with the invention of carbonless receipts and carbons that tear in half, the carder is less likely to find a good number in a trash can (you can bet on getting dirty). But some stores make the fatal mistake of not ripping up their fuck ups. A fuck up is when they run the card number thru with the wrong amount or the lady (it's always a lady) decides to pay cash. The clerk throws the credit voucher into the trash, and that makes its way out to the bin where we find a plethora of "fuck ups". The best way to get a number is off of an actual card. If you are at a store where they take credit cards, watch someone pay, and copy his/her number down on a business card you just happen to have. This may seem risky, but trust me, IT'S NOT!! A third way that is not always as effective is to hunt mailboxes at night, Sometimes people forget to get their mail, and inside there will be a bill from Visa or Bank of America (don't forget that banks offer credit cards now). If you're real lucky, you'll get an actual card. Okay, now you've got your card:

CARDING!!!!

Find a little shit mail order company that has put out a small add in crumby production like Nuts & Volts magazine. Call this number up and say "I'd like some information on XXXXXXXXXX", where XXXXXXXXXX is the item you wish to get for free. Continue to ask questions and TRY TO BARGAIN. This is important because people who are spending their own money try to get the best deal POSSIBLE.

Finish the conversation by saying "Okay, let me look around and try to find the best price." The salesperson will give you their name and ask you to call back. Call back the next day, and continue to BS before ordering. Once you have ordered, they will ask you for: The card number, the name, the expiration, the mailing address (always use a drop site, and when they say "Is this the address as it appears on the card?" Say yes even if it isn't), and a phone number. The best phone number to give is one that is always busy or that of a hacked VMB. Ask for next day delivery on all packages. Now you need to send it somewhere.

DROP SITES

A drop site is the address you want your package sent to. The best type of drop site is that of a vacant house, or where your neighbor is outta town. Some say to leave a note on the doorstep asking the UPS dude to leave the package, but some companies require a signature. Here's my plan: Stay close to the house you pick for a drop. When you see the van pull up, walk non-chalantly over to the delivery man and say "My neighbor asked me to pick this up for him". Sign a fake name and walk away. Now you have your package!!!!

P/HARM Conquests:
Dual Standard HST
661 megabyte hard drive (SCSI)
330 megabyte hard drive (SCSI)
Laptop computer (Pending)
330 megger SCSI (Pending)

****
* DISCLAIMER!!!!!!!! *
****

This file is written as a means of information interchange only. If you choose to try the methods described above, well that is by your own choice, and I nor P/HARM will be held responsible for any trouble you get yourself into. **REMEMBER carding is ILLEGAL!!!

****
* DISCLAIMER!!!!!!!! *
****

Information on how to card!

First of all, you need a good drop site. A drop site is a place where you are going to have the package shipped to. The best

places are usally private homes where people work during the day. A easy to way to get one, walk out your house and look around. Find any house,write down the street address. Open up a yellow pages,look for the fone #. Then call up the house, usally during morning time. If there is no answer,well you got a drop site. Next,you need a card. Humm, usally the best way to get cards is trough CBI or TRW. I used to use a program called checksum. Its a program that makes CC's. Then I would call 800 # card checker. Put a $150 ammount on the card,if it was aproved then you got a real card. I am not going to tell ya how to get cards. Next, open up any computer realated magazine. Look for small ads, preferbly in the west coast. Call 'em up, see if you sound like chinks, if they do then you may have found a good place. Once you have the neccesery items you are ready to CARD.

The following things are needed to get away with carding.

1. A good unused card.
2. Drop site.
3. Cheap copmany to order from.
4. A code to call them with.
5. A loop for reciving fone calls.

Ok. you call up the fuckers. And you talk to some rep.

I am going to help ya all get 14.4's. When you talk to the rep. use the following lines to why you need a 14.4

1. My modem was fried by lighting,and I am in need of very importent docs. 2. I am looking to upgrade the modem at the office,I only have a 1200 baud.
3. Its a holiday,birthday whatever. You want to get a gift for you son.

Ok. Next, make sure you ask for the price,any discounts on it,what does it come with. Also make sure you tell them that you want to know what you can do incase the modem doesnt work. Ok,Then say "Ok,

I will order this now". Then she starts asking questions. Usally they ask for the name first. Now, I never ONCE had a real name for all my cards. Thats why I told you to order from small companies. Make up any name in the fuckin world. But write it down to remember it later on. Then they will ask you for a shipping address. Give them the address of the drop site. Say thats were you live and you are sending it to your house. Next, they will ask for the card #. Geeeeee, Give them the card #. Now, they will want an experation date. People tell me that need a experation date. BULLSHIT!!. You do not need an exp. date at all. Give them, any thing. But make sure its with in a year or two. Not 1/96. use like 1/91 1/92 etc.. OH yeah. When they ask for the card #. I allwayes say "Hold on, lemme get my wallet out". That makes it look like you are getting the card out from your wallet, GEEE. Humm,Now they want a phone #

This is a bitch. Up untill a few months ago, I used to give them a BBS thats allwayes busy. That works sometimes , but the best is to use the following methood. Get a LOOP.

And say you are currently at a hotel in the loops area code. Then say you want to go out and play raquetball or something at the hotel. So you are not going to be around. Then ask them when are they going to call back and shit. Sometimes if you are sure the card is going to work, you can say if everything is ok, then ship it. I sometimes use this; I say "My wife got a hold of my card and went shopping, so I am not sure if the limit on the card can hold it." then I say "Can you check to see if it gets approved while I'll wait online". Most of the time they will "OK, hold on". Sometimes they can say it takes a while. Who cares, just say "I am stepping out to lunch now, can I give you a call back to check if every-thing is ok". And they say thats fine. Make sure you dont fuck up. And dont try to card if you have the voice of a 13 year old. My friend has the voice of a kid and he got caught HIS FIRST TIME CARDING BY THE FEDZ!!!!. So do not card if you are a little kid. After you are done giving the bitch all the info. Ask to have it shipped NEXT DAY SERVICE (RED LABEL). That way you dont have to wait a week or so. And then you have more time hidding and shit. Its a little bit more,but who gives a fuck. Make sure you ask how much is for everything!!!. And when you are about to hang up. Make sure you say thank you, Have a good day. it makes a good impresion of them. And remember try NOT to order from 800's. Allwayes CALL WITH A CODE. That way if you get fucked, they cant prove you called the place and shit. Well, I am done for now. I think, I dunno. Remember if you use this file and get shit, lemme know. I want to know if I helped people card shit. Hehehehehhe. Me personaly have carded more shit then your parents make in a year and shit. And still do. I dident get caught yet. But I am going to be 18 so, and then I will be of probation (Not for carding). So , if you are under 16 card card card! they cant do shit to you....

Advanced Carding Techniques

CARBONS:

Remember trash-picking the department store to find those little black pieces of paper that "told all" for the CC number? Well, kiss that old technique goodbye, the newest thing on the market that will soon be widespread is SELF CARBONING RECIEPTS. Those do just what they say. The "carbon" is part of the paper itself. You then have the customer copy, and the store copy, and thats it, nothing else. The best way to get numbers anymore is to get them from the place you work at.

DROPS:

Drops are as easy as they ever were, but with a few changes. Remember how the place you call would ask you "What number can we reach you at?" You would just give them the phone number of a payphone that you were at, and maybe they would call you in a few minutes to verify the order. Now they always ask this "What is your home telephone number?" To have a successful shipment, you *MUST* give them the correct phone number to the house that you are having the stuff sent to. This *MUST* corrispond! What they do is this, lets say that you give them this info:

Jim R. Jnes
132 S. Alexander
Arlington Hts, IL 60002
Home: 312-962-3342
Work: 312-564-1233 (Don't worry about this, give 'em a carrier #)
Visa: 4432-432-223-032 6/86
Bank: Second National Bank

They will then call the 312 Directory Assistance (312/555-1212) and say something like this: "I would like the number for the JONES residence on South Alexander-" and then the operator would either say the number, or that she can't give it out. If the operator says something to the effect of "I'm sorry, but I have no listing of a JONES at this number, then your fucked, cause the store will figure that its a fraud order, and sometimes will call VISA. Make sure that the phone corrisponds with the drop!

CHECKING CC'S:

Go to about any store that uses credit cards, and look at the thing that they run the credit cards through to make the carbons. On that thing there will be an 800 number and some special numbers. Write all these down! Ever have it where you use a card number and it doesn't work out, and you want to check to see if the card number is still good? Well, this is how you use those beloved numbers you have!

Call th 800 number, a lot use this numbers:
800-221-1122 and along with those numbers you sould have found a 4 digit number and one that is long as all hell, sometimes over 10 digits long. The first number (the short one) is the BANK number, and the other long one is the MERCHANT NUMBER. Call the 800 number and they will usually answer with something like:

"National Data"

Say: "Bank number 1122" <==or whatever # it was
(pause, let the bitch type)

Say: "erchant # 541837265355" <==whatever #
(pause)

Say: "Crd number 44312-223-433-221 exp 6/86"
(pause)

Say: "Amount is $12.31"
Note: Always try to keep this number low, for
credit sake!

If the card number is still good she will say something like: "ok, that is authorization #4423B" (or something like that) Don't worry

about this number, all you need to know is that the number is still valid. Sometimes is the number is bad, you'll hear: "Let me repeat that number" (and she does) then she says: "That card is a pick up" This means that they know it is a stolen card number and if you can get ahold of the original card, a storeowner can get $50. All this means to you is that you can cross that number off your list.

THINGS TO CARD-THINGS *NOT* TO CARD:

I have carded at great number of things on my life, and I have found that computer equipment is one of the hardest things to card, 'cause think about it, almost everyone who cards, will card a new Apple Cat, or something like that. Stay away from the computer stuff as much as possible, these are checked *VERY* well! Jewrey is also hard to get because its so easy to resell! I once orderd a Rolex watch on my own American Express Gold Card, and it took a WEEK for them just to preform the credit check to make sure it was really my card! They laughed when I said that I wanted to pay for it by credit card, they only had 1 CC order in the past 8 months! This was a high volume store, too! Anyways, hold of on the diamonds, Gucci or Saks stuff, they check too much!

Airlinetickets are the easiest to card by far, and stereo equipment too! I not to long ago got a Nakamichi Dragon cassete deck, which is one of the best cassete decks in the world, and cost in excess of $1000! I ordered it on a Monday, and it came on Thursday! Try to make friends with the guys your order from, say bullshit like:

"I'll cll you when I get it and tell you how it works out!!!"

I have been really successful with this, and these tips should help you!

Airlines:

Everybody travels, and flying is the only way to go, but lets face it, nobody ever has enough money to fly quite as often as we would like. This is where carding can save you money and let you do the things that you really want to do!

Getting Tickets:

I am assuming that you already know how to get carbons, etc. OK, you have this stack of carbons w/ good card numbers. Next grab the phone (and phone book). Look up AIRLINES. Call your favopite airline and schedual yourself (under a John Doe name, of course.) You could do this actually long in advance, to "save" Visa some money, and maybe make it look a little more ordinary. Fdw people take off to Rio, Brazil without planning ahead! A few days (I'm talking 2 or 3 days AT THE MOST) before your flight is going to leave, call up a local travel agency, but CALL THEM THROUGH AN 800 EXTENDER! Find one with the WORST connections possible, a PBX might work great. You want the agency to think that you are not calling local, but from across the country. Tell the lady at the agency that your son goes to college (or something) is flying down, and that you have made reservations for him to fly back. ONLY BUY ONE-WAY TI CKETS! Tell them that you already have reservations. The agency will be cool about it all, and will take your card number and all the usual info. Tell them that your son is supposed to call you a little later, and that you will tell him to go down and pick up his ticket.

The key to the whole deal is that 800 extender. This makes the agency think that there really is a father in New Jersey that wants his son to be flown from Bakersfield to Chicago to see his brother.

It really is that easy to do, but as I said, do not get round trip tickets. Let's say that you do and fly to wherever, and while you are there, the guy's Visa bill comes. The airport may have some people waiting for you when you get on! The best bet is to take a stack of carbons and extenders with you and do the same thing to get back.

This is the way I have flown and I have never had any problems, whatsoever.

Basic Information About Credit Cards

There are at least three types of security devices on credit cards that you aren't supposed to know about. They are the account number, the signature panel, and the magnetic strip.

The Account Number

A Social Security card has nine digits. So do two-part Zip codes. A domestic phone number, including area code, has ten digits. Yet a complete MasterCard number has twenty digits. Why so many? It is not mathematically necessary for any credit-card account number to have more than eight digits. Each cardholder must, of course, have a unique number. Visa and MasterCard are estimated to have about sixty-five million cardholders each. Thus their numbering systems must have at least sixty-five million available numbers. There are one hundred million possible conbinations of eight digits-- 00000000, 00000001, 00000002, 00000003, all the way up to 99999999. So eight digits would be enough. To allow for future growth, an issuer the size of Visa of MaserCard could opt for nine digits---enough for a billion differnt numbers. In fact, a Visa card has thirteen digits and sometimes more. An American Express card has fifteen digits. Diners Club cards have fourteen. Carte Blanche has ten. Obviously, the card issuers are not projecting that they will have billions and billions of cardholders and need those digits to ensure a different number for each. The extra digits are actually a security device. Say your Visa number is 4211 503 417 268. Each purchase must be entered into a computer from a sales slip. The account number tags the purchase to your account. The persons who enter account numbers into computers get bored and sometimes make mistakes. They might enter 4211 503 471 268 or 4211 703 417 268 instead. The advantage of the thirteen-digit numbering system is that it is unlikely any Visa cardholder has 4211 503 471 268 or 4211 703 417 268 for an account number. There are 10 trillion possible thirteen-digit Visa numbers (0000 000 000 000;0000 000 000 0001;... 9999 999 999 999). Only about sixty-five million of those numbers are numbers of actual active accounts. The odds that an incorrectly entered number would correspond to a real number are something like sixty-five million in ten trillion, or about one in one hundred and fifty thousand. Those are slim odds. You could fill up a book the size of this one {note, book is 228 pgs long} with random thirteen-digit numbers such as these:

3901 160 943 791
1090 734 231 410
1783 205 995 561
9542 425 195 969
2358 862 307 845
9940 880 814 778

8421 456 150 662
9910 441 036 483
3167 186 869 267
6081 132 670 781
1228 190 300 350
4563 351 105 207

Still you would not duplicate a Visa account number. Whenever an account number is entered incorrectly, iw will almose certainly fail to match up with any of the other account nubmers in the computer's memory. The computer can then request that the number be entered again. Other card-numbering systems are even more secure. Of the quadrillion possible fifteen-digit American Express card numbers, only about 11 million are assigned. The chance of a random number happening to correspond to an existing account number is about one in ninety million. Taking into account all twenty digits on a MasterCard, there are one hundred quintillion (100,000,000,000,000,000,000) possible numvers for sixy-five million card-holders. The chance of a random string of digits matching a real MasterCard number is about one in one and a half trillion. Among other things, this makes possible those television ads inviting holders of credit cards to phone in to order merchandise. The operators who take the calls never see the callers' cards nor their signatures. How can they be sure the callers even have credit cards? They base their confidence on the security of the credit-card numbering systems. If someone calls in and makes up a creditcard number--even being careful to get the right number of digits--the number surely will not be an existing real credit-card number. The deception can be spotted instantly by plugging into the credit-card company's computers. For all practical purposes, the only way to come up with a genuine credit-card number is to read it off a credit card. The number, not the piece of plastic, is enough.

Neiman-Marcus' Garbage Can

The converse of this is the fact that anyone who knows someone else's card number can charge to that person's account. Police sources say this is a major problem, but card issuers, by and large, do their best to keep these crimes a secret. The fear is that publicizing the crimes may tempt more people to commit them. Worse yet, there is alomost nothing the average person can do to prevent being victimized {muhaha} -- short of giving up credit cards entirely. Lots of strangers know your credit-card numbers. Everyone you hand a card to--waiters, sales clerks, ticket agents, hairdressers, gas station attendants, hotel cashiers--sees the account number. Every time a card is put in an imprinter, three copies are made, and two are left with the clerk. If you charge anything by phone or mail order, someone somewhere sees the number. Crooks don't have to be in a job with normal access to creditcard numbers. Occasional operations have discovered that the garbage cans outside prestige department or specialty stores are sources of high-credit-limit account numbers. The crooks look for the discarded carbon paper from sales slips. The account number is usually legible--as are the expiration date, name, and signature. (A 1981 operation used carbons from Koontz Hardware, a West Hollywood, California, store frequented by many celebrities.) Converting a number into cash is less risky than using a stolen credit card. The crook

need only call an airline, posing as the cardholder, and make a reservation on a heavily traveled flight. He usually requests that tickets be issued in someone else's name for pickup at the airport (airlines don't always ask for ID on ticket pickups, but the crook

has it if needed) and is set. The tickets can be sold at a discount on the hot-ticket market operating in every major airport. There are other methods as well. Anyone with a Visa or MasterCard merchant account can fill out invoices for nonexistent sales and submit them to the bank. As long as the account numbers and names are genuine, the bank will pay the merchant immediately. For an investment of about a thousand dollars, an organized criminal operation can get the pressing machines needed to make counterfeit credit cards. Counterfeiting credit cards in relatively simple. There are no fancy scrolls and filigree work, just blocky logos in primary colors. From the criminal's standpoint, the main advantage of a counterfeit card is that it allows him to get cash advances. For maximum plundering of a line of credit, the crook must know the credit limit as well as the account number. To learn both, he often calls an intended victim, posing as the victim's bank:

CROOK: This is Bank of America. We're calling to tell you that the credit limit on your Visa card has been raised to twelve hundred dollars.
VICTIM: But my limit has always been ten thousand dollars.
CROOK: There must be some problem with the computers. Do you have your card handy? Could you read off the embossed number?

On a smaller scale, many struggling rock groups have discovered the knack of using someone else's telephone company credit card. When a cardholder wants to make a long-distance call from a hotel or pay phone, he or she reads the card number to the operator. The call is then billed to the cardholder's home phone. Musicians on tour sometimes wait by the special credit-card-and-collect-calls-only booths at airports and jot down a few credit card numbers. In this way, unsuspecting businesspeople finance a touring act's calls to friends at home. If the musicians call from public phones, use a given card number only once, and don't stay in one city long, the phone company seems helpless to stop them. What makes all of these scams so hard to combat is the lead time afforded the criminal. Theft of a credit card--a crime that card issuers will talk about--is generally reported immediately. Within twenty-four hours, a stolen card's number is on the issuer's "hot list" and can no longer be used. But when only a card number is being used illicitly, the crime is not discovered until the cardholder recieves his first inflated bill. That's at least two weeks later; it could be as much as six weeks later. As long as the illicit user isn't too greedy, he has at least two weeks to tap into a credit line with little risk.

The Signature Panel

You're now supposed to erase the signature panel, of course. Card issuers fear that crooks might erase the signature on a stolen credit card and replace it with their own. To make alteration more difficult, many card signature panels have a background design that rubs off if anyone tries to erase. There's the "fingerprint" design on the American Express panel, repeated Visa or MasterCard logos on some bank cards, and the "Safesig" desgn on others. The principle is the same as with the security paper used for checks. If you try to earse a check on security paper, the wavy-line pattern erases, leaving a white area-- and it is obvious that the check has been altered. Rumors hint of a more elaborate gimmick in credit-card panels. It is said that if you erase the panel, a secret word--VOID--appears to prevent use of the card. To test this rumor, fifteen common credit cards were sacrificed. An ordinary pen eraser will erase credit-card signature panels, if slowly. The panels are more easily removed with a cloth and a dry-cleaning fluid such as Energine. This method dissolves the

panels cleanly. Of the fifteen cards tested, six had nothing under the panel(other than a continuation of the card back design, where there was one). Nine cards tested had the word "VOID" under the panel. In all cases, the VOIDs were printeed small and repeated many times under the panel. The breakdown:

Void Device	Nothing
Bloomingdale's	American Express Gold Card
Bonwit Teller	Broadway
Bullock's	MasterCard(Citibank)
Chase Convenience B.C.	Neiman-Marcus
I. Magnin	Robinson's
Joseph Magnin	Saks Fifth Avenue
First Interstate B.C.	
Montgomery Ward	
Visa (Chase Manhattan)	

When held to a strond light, the VOIDs were visible through the Blooming-dales's card even without removing the panel. The VOID device isn't foolproof. Any crimianl who learns the secret will simply refrain from trying to earse the signature. Most salesclerks don't bother to check signatures anyway. Moreover, it is possible to paint the signature panel back in, over the VOIDs--at least on those cards that do not have a design on the panel. (Saks' panel is a greenish-tan khaki coler that would be difficult to match with paint.) The panel is first removed with dry-cleaning fluid. The back of the card is covered with masking tape, leaving a window where the replacement panel is to go. A thin coat of flat white spray paint simulates the original panel.

The Magnetic Strip

The other security device on the back of the card, the brown magnetic strip, is more difficult to analyze. Some people think there are sundry personal details about the cardholder stored in the strip. But the strip has no more information capacitythan a similar snippet of recording tape. For the most part banks are reticent about the strip. The strip need not contain any information other than the account number or similar indentification. Any futher information needed to complete an automatic-teller transaction-- such as current account balances--can be called up from bank computers and need not be encoded in the strip. Evidently, the card expiration date is in the strip. Expired cards are "eaten" by automatic-teller machines even when the expired card has the same account number and name as its valid replacement card. Credit limit, address, phone number, employer, etc, must not be indicated in this strip, for banks do not issue new cards just because this info changes. It is not clear if the personal identification number is in the strip or called up from the bank computer. Many automatic-teller machines have a secret limit of three attempts for provideing the correct personal identification nubmer. After three wround attempts, the "customer" is assumed to be a crook with a stolen card, going through all possible permutations--and the card is eaten. It is possible to scramble the information in the strip by rubbing a pocket magnet over it. Workers in hspitals or research facilites with large electromagnets sometimes find that their cards no longer work in automatic-teller machines. (If you try to use a magnetically doctored card, you usually get a message to the effect, "Your card may be inserted incorrectly. Please remove and insert according to the diagram.")

The Bloomingdale's Color Code

Only in a few cases does the color of a credit card mean anything. There are, of course, the American Express, Visa, and MasterCard gold cards for preferred customers. The Air Travel Card comes in red and green, of which green is better. (With red, you can charge tickets for travel within North America only.) The most elaborate color scheme, and a source of some confusion to status-conscious queues, is that of Bloomingdale's credit department, here is how it works: Low color in the pecking order is blue, issued to Bloomingdale employees as a perk in their compensation packages. The basic Bloomingdale card is yellow. Like most department store cards, it can be used to spread payments over several months with the payment of a finance charge. The red card gives holders three months' free interest and is issued to customers who regularly make large purchases. The silver card is good for unlimited spending, but as with a travel and entertainment card, all charges must be paid in thirty days. The gold card offers the same payment options as the yellow card but is reserved for the store's biggest spenders.

♠

Card Formats and Bank Numbers

I. PREFACE

This is my first infofile as a N.A.R.C. member. For those of you who have read "Getting Serious about Carding by Optical Illusion", this is a somewhat a con-tinuation of things you need to know about carding which Optical Illusion did not cover. In this file, we'll try to cover the aspects of the use (or shall we say misuse) of a credit card, strategies mail order companies keep us from getting away with carding, and a list of bank id numbers with their banks.

II. CREDIT CARDS versus CHARGE CARDS

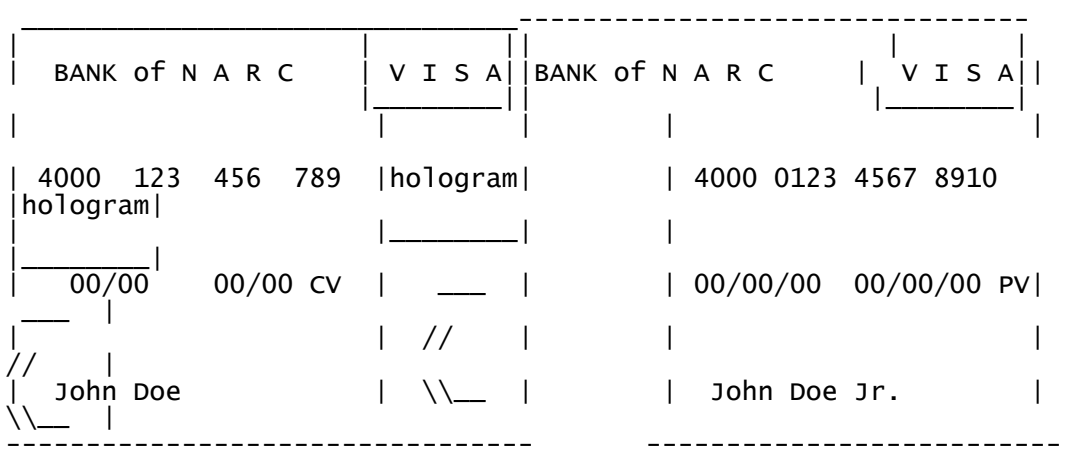
Many people have the misconception that all cards are credit cards. This is of course not true. For example, American Express is a charge card and not a credit card. American Express is a charge card since the owner of the card must pay off the whole amount when his bill comes. If the owner doesn't, he or she is in serious shit. One thing good about the American Express is that it has no limit on how much the person can spend as long as the person can pay off the bill when it comes. Basically, the card is based on the person's good judgement on how much money the person have. Why is there American Express Gold and regular American Express cards then? It still has a hidden limit which you cannot buy a Corvette ZR-1 with a regular American Express. You could however do it with a American Express Platinum (if you can find one to abuse). This means you can buy more expensive things at one time with a Gold or Platinum card. Credit cards have a set limit after you you apply for the card. Usually a Classic Visa has about $700 plus or minus $100. Mastercard on the other hand has about $1000 limit on it.

III. TYPES OF CARDS

Credit Cards	Charge Cards
VISA	American Express
Mastercard	American Express
Optima	
Discover	

Here's a couple type of cards I do not know what category they fall into since they are never accepted by mail order companies. One of them is Diner's Club International and the other is Carte Blanche.

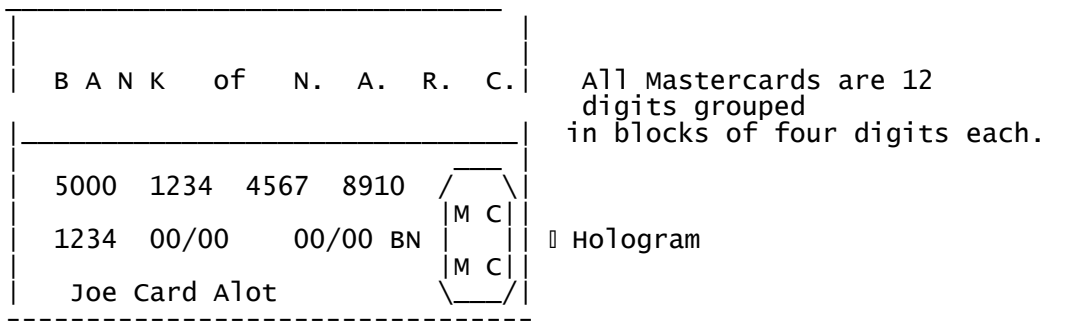
Bank name



Bank name

VISAs are grouped either in 4XXX XXX XXX XXX or 4XXX XXXX XXXX XXXX. The 2 groupings used are different for each bank. There are banks' (regular) Preferred (better, much better) preferred cards that are group in 4 3 3 3.

This is either a C or a P.
C for Classic
P for



All Mastercards are 12 digits grouped in blocks of four digits each.

Hologram

BN is the Bank initials

1234 is the bank id number.
The bank may have more than one id number for their 5000 XXXX XXXX XXXX series cards.

IV. MAIL ORDER COMPANIES

Most of the mail order companies will accept Visa or Mastercard. Some will also accept American Express and Discover. These mail order companies check the card by either calling into a TRW center to check if the amount of the order will exceed the limit. In either case of a approval or declining, the mail order companies will call you back to check with you the order you have placed. Anyways, a way of finding a valid card is to call a credit approval system yourself. Here's some ways of checking:

(1) 1-800-554-2265 for check Mastercard or Visa

for Visa 20#1067#24#CARD#EXP#XX*XX#

- 10 and 20 are for the type of cards
- 1067 is the bank id number
- 24 is the merchant number (52 will also work)
- EXPiration must be in the form of 0291 for feb of 1991
- XX*XX is the amount. Use a small number like 11*04 for $11.04.

Another way mail order companies verifying cards is to call the bank of the card and verify the name of the person and the billing address versus the name you gave the mail order companies and the address (drop site). So the only way of getting pass this is to have the stuff sent to the person's address or getting the waybill number from the mail order houses and intercept the package at the UPS or Federal Express office before the package arrive's at the card owner's address.

V. VISA BANK Numbers

4428 Bank of Hoven
4128 Citibank CV
4271 Citibank PV
4929 Barclay Card CV (from England)
4040 Wells Fargo CV
4019 Bank of America CV
4024 Bank of America PV
4019 Bank of America Gold (This card looks like a CV but without a CV afterthe expiration date)
4678 Home Federal
4726 Wells Fargo CV
4036 4561 4443 4833 4070 4735 4673 4044 4050 4226 4605 4923 4820
4048 CV 4121

VI. Mastercard

A. BANK NUMBERS

5419 Bank of Hoven
5410 Wells Fargo
5412 Wells Fargo
5273 Bank of America Gold
5273 Bank of America
5254 Bank of America
5286 Home Federal
5031 Maryland of North America
5326 5424 5250 5417 5215 5204 5411 5421 5329 5308 5217 5415

B. BANK ID NUMBERS

5410 Wells Fargo -- 1037
5410 Wells Fargo -- 6785
5419 Bank of Hoven -- 1933
5410 Wells Fargo -- 6037
5204 -- 1006
5250 -- 1260
5215 -- 6207

5424 -- 1065
5411 -- 1169
5421 -- 2143
5417 -- 1786
5417 -- 1711
5415 -- 1530

VII. AMERICAN EXPRESS

3728 GOLD
3713 Regular
3732 Regular

3737 3782 3731 3724 3742 3727 3787 3726 3766 3734 3749 3763 3710 3718 3720 3739

Carding For Benfit And Profit

First off, there are many types of credit cards. But the main ones we will be discussing are American Express, Discover, Mastercard, and Visa. These four are the largest and most widely used types. My personal favorite is the Discover card, since the company is a real loser. It is best for the beginner to start out with Discover, then move to American Express, then to Mastercard, and finally visa,

The first thing you have to do is to find a credit card number (we will be refering to them as CCNs). There are several different ways of going about this, which will be discussed later in this file. The way you can tell the cards apart are the first digit of the CCN.

Digit	Type of Card
3	American Express
4	Visa
5	Mastercard
6	Discover

Now that you know the first digit of the card you want you need the different CCN formats. They are listed below.

American Express

3xxx-xxxxxx-xxxxx

Visa

4xxx-xxxx-xxxx-xxxx

or

4xxx-xxx-xxx-xxx

Citibank Visa, which is by far the most popular is

4128-xxx-xxx-xxx

Mastercard

5xxx-xxxx-xxxx-xxxx

The type of Mastercard I use is Citibank which is

5424-xxxx-xxxx-xxxx

Discover

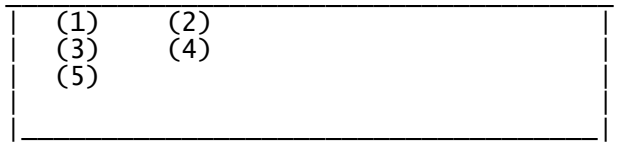
6xxx-xxxx-xxxx-xxxx

There are a number of ways through which you can get CCNs. They are listed below in order of easiest method to hardest method.

1) Go for a little swim. That is, in a big dumpster. This is called trashing. Go in back of department store or anywhere that accepts credit cards and jump in. But make sure it's not at a mall, or

someone might see you and contact the police. When you've found the perfect dumpster, just dive right in. Just look around for carbons. You know, the things that the salesperson throws away after a credit card purchase. If anyone sees you, just pretend you're a bum. Or if that won't work, pretend you're looking for your baseball that flew in. Once you find these, (and making sure you don't rip them) put them in your cap, or somewhere where they won't fall out, and just calmly go home. Now comes the easy part. You just copy down everything important. The CCN, Expiration date, and Name. Then you rip it up into shreds and burn them. Now there is no way you can get caught unless you're a REAL idiot. 2) If you have a friend (it's better if it's a fellow pirate) that works in a store which performs credit card transactions, you might save yourself the trouble of trashing and ask him if he doesn't mind slipping some carbons into a bag after they ring up a sale. If he won't, bribe by saying you'll get him something too.

Carbons



(1) The Account Number. This is the most important thing on a Credit Card. (2) The Expiration date for Visa or Mastercard (3) The Expiration date for Visa or Mastercard (4) The Expiration date for American Express (5) The Card Holder's name. The name is not very important but it is good to have. 3) If are really advanced, you can use a credit card formula, several do exist. If you're good at math and patterns, you should be able to figure out at least one formula. Once you have a newly formulated or newly found Credit Card, you have to first check to see if it is still valid before you try to use it. The easiest way I know of, is 1-800-554-2265. But after you enter something you must enter a pound. Just look at the example if you're confused. You must first, of course, dial 1-800-554-2265. Then it should say "Enter type".

Number	Card Type
10#	Mastercard
20#	Visa
30#	American Express

Then it will ask you for "Bank identification". Just enter 1067#. Now it will request a Merchant Number. Enter either 24# or 52#. Either one should work. Now it will ask you for the card number. Enter it in with a # sign following it. Then it will ask for the expiration date. Enter it with a # sign following it. And last,

but not least, it will ask for the amount. This is a little

rickier. Look at the examples. If you still don't understand it, hen you're dumb, and you shouldn't be trying to card. For $100.25 ou enter 100*25#. For $1,532.67 you enter 1532*67#. Got it? Good. ow the moment of truth comes. In the next few seconds the computer will say Approved or Declined. Yes or No. Light or Dark. If it's approved, pat yourself on the back. If not, too bad. Go look for another one.

* SPECIAL NOTE *

In Canada dial 416-785-3222 for Visa credit checks or dial 1-800-268-2439 for Mastercard credit checks. For a Visa credit check in Canada, you first dial the authorization center and a operator will answer. Then you will be ask for the card number, amount of purchase, merchant # and expiry date. If the card is good then she'll tell you the authorization number. If the card is invalid then she'll say that the number was invalid. For a Mastercard credit check in Canada, you first dial the authorization center and a automated computer will answer. It will ask you if you want it in French or English, so if you want English punch in 1, or if you want French punch in 2. Next it will ask you for the "Credit Card Number". Just punch in the Mastercard number and the press the # sign following the number. Next it will ask you for the "Amount In Dollars Only", so press in the amount and then the # sign following it. Next it will ask for a "Merchant #", this can be skipped by just pressing the # sign. After that it will ask for a "Expiry Number". Punch the expiry number in and press a # sign following it, if you made a mistake punching in the amount, then from here you press 2 and change the amount of the purachse. After all that it will come back and if it's valid, it will tell you an authorization number, otherwise it will say that the number was invalid. If the amount is too high, then it will tell you to hold on for an operator. And then the operator will verify the card for you.

****

ONE NOTE: IF A CARD HAS $5000 AND YOU VERIFY IT FOR $3000 DOLLARS, YOU CAN ONLY VERIFY IT FOR $2000 MORE. ANOTHER EXAMPLE IS IF THE CARD HAS $3000 AND YOU VERIFY IT FOR $1250, THE CARD CAN BE VERIFIED $1750 MORE BEFORE IT WILL SAY DECLINED.

****

Now for the hardest part of all, purchasing merchandise with your newly verified CCN. You will probably want some computer equipment, knowing that that's what most people want. And be sure to read this entire file before attempting to card something. If you don't, you might get caught and spend ten years in jail and never be able to get another decent job again, just because you didn't listen to me and read this entire file. Now that I have your attention, we must lay down some rules for ordering merchandise to insure your safety. 1) Always go to a pay phone.

2) Never give out your real name. 3) Or your address and telephone number. 4) Plan out the drop site and the fake number. I use the busiest PD board there is. 5) Sound calm. Remember, they can't do anything to you. 6) If they get suspicious, just keep sticking to the same story. A consistent lie is better than a inconsistent truth. Where should I ask them to ship it to? This is a common question. The best place to have the merchandise shipped to is an abandoned house. The sites where you want them shipped are called drop sites. Jot down this address. Now that we have set those rules, we now have to call a store. Make sure it is a small store, for they don't have the card checking techniques the bigger ones do. Now when they ask you your name and stuff like that, just give them the fake ones, without hesitation!! If you hesitate then they might get suspicious. Even spell it out for them. And try to be friendly. Don't sound nervous or anything. Now if they are online to credit bureaus suck as CBI or TRW then make up an excuse, like have your friend

threaten you in the background (or something). If they are online with CBI or TRW they can verify everything in just a couple of minutes. Now if they aren't then you're in luck. Now when they ask for a number, give them the number you have ready. Bullshit your way through. If they aren't online, they can't verify really anything but that the CCN is valid and there is enough credit to pay for the merchandise. I wouldn't suggest making a business out of this, either. Sure, if you want to get a few dollars for things you order (and that you don't want anymore) sell it and keep the money. It wouldn't be all that great to go to jail for ten years and never get another decent job in your whole entire stinking life, just because someone you don't even know, wanted a bigger hard drive for $100? Yeah, you know I have a good point there. Well, the truth is that the only people that should really even make deals are the people with lots of experience.

And now how to card Travelers Checks. These are alot easier than what I just talked about. All you gotta do is call 1-800-777-7337 and use an American Express card and ship it to your drop site. Now just go to another country and spend away. Have fun. Now for the most dangerous way of carding, by far. In person carding. But you get the stuff really quick. Now you need a fake name again. This time you need two. Your dad and a son. Lets say your name is Robert Armstrong. Look at the example.

"Hello, Computers for less, how may I help you?"

"Yes, this is Robert Armstrong calling from California (or somewhere across the country). My son, Mike, needs an Apple II. It says here in your ad that you sell them for such and such. I would like to place an order for one."

"OK. And how will you be paying for this?"

"Visa."

"OK. Number?"

"4xxx-xxxx-xxxx-xxxx."

"OK, thank you. Now how do you want this shipped?"

"Well, since my son is going to college right next to you, I thought I could send him to go pick it up."

"Oh, OK. Sure. Do you want us to call your son to notify him?"

"No, that's ok. He's supposed to call in a couple of minutes. He always calls me at 5:00PM every Friday. I can't wait to hear what he says when he hears what I got him. When can he go pick it up?"

"Anytime."

"Ok, thank you.

"Thank you for ordering from Computers for Less."

<CLICK>

Now comes the most dangerous part. Go to the store, park your car where none of the employees can see it. Now go in and state your fake name and what you are there to pick up. In Mike's case...

"Hello. I'm here to pick up an Apple II my dad bought for me."

"OK, sure. Mike Armstrong?"

"Yes, that's me."

"Ok, wait. We'll bring it up right now."

"Thank you."

"Well, here you are."

<TAKE>

"OK, Thank you."

"No problem. Thank you for ordering from Computers for Less."

Now just walk over to your car and drive off. I wouldn't really recommend this method, but if you're desperate, try it. Now if they get suspisious, don't get nervous. Just start complaining. Say like "My dad paid good money for this system and now you won't give it to me?" If they still won't give it to you, then say, "Ok, I'll come tommorrow. But if it isn't ready tommorow I'm going to tell

my dad to get a refund." Then walk out really pissed looking and never go back. They were probably setting up a trap for you. Better safe than sorry. Now I'll explain what happens to the unlucky guy. The guy's CCN you used of course. Now let's pretend this unfortunate soul's name is John Doe. At the end of the month, John Doe gets his Visa bill from the bank's credit card department. Among the things on his bill he notices a VGA card and monitor. John Doe then calls his bank and starts cussing them out and asking where the fuck did they get the VGA card and monitor from. Then the bank should send him a xerox copy of the original reciept, showing when it was bought and where it was sent to, and the second is an affidiate. This is a formal document saying that you did not make the purchase, you do not know who did, and did not authorize this purchase. It must be signed by him and then brought to the bank and signed by a notary public and have the bank's stamp on it. From there the bank can either go to their insurance agent or Visa, depending on who they have a deal with, and be paid for the carded stuff. Then John Doe must cut his cards in half and send them to the bank. After he has done that, he is re-issued new cards with a new CCN.

How to Find Credit Cards: carbons or other methods

II. Trash Digging

Although not the most fun method of getting CCs it is the safest by far. It does not take much intelligence to go through a dumpster and look for credit card carbons... But I assure you even the most experienced carders use this method. The way this is done is to find a store that people always or almost always use credit cards. It must also have a dumpster or trashcan where its garbage is dumped that is out of plain sight. Wait for the store to close or go when few people are around and search for ripped up carbons. Then piece them together and you should get full or partial information.

III. Slight of Hand

Another method which I myself often use is this trick on ususpecting customers...If you work as a cashier at a store that accepts credit cards you have an excellent opportunity to get card numbers and full info. What you need to do is when someone comes in and buys something via credit card, you wait for him/her to rip up the carbon and throw it out, if he/she throws it out in the stores trashcan, pick up the cardbon right away. Or sometimes the person will not even ask for his/her carbon, although this is somewhat rare.

But I have even had someone leave their actuall credit card behind, then I just copy the name and number down, and give it back.

IV. Mailbox Searching

This is basically a very lame way to get credit cards due to the danger and in order to get CCs this way you get the actuall card. What you do is have a bunch of pointless flyers made up, and goto a decent neighborhood away from your area of residence that has homes with accesable mail boxes. Wear sunglasses and a baseball hat if possible, although don't wear the shades on a cloudy day. Do this during school time if possible so you are not seen. What you do is go by each persons mail box and put a flyer in it (Which in itself is illegal, but few people know this) and while you are doing so search the mail for envelope from banks. If you happen to find one from a bank slip it into your pile of flyers and sneak off to open it. If it has a CC in it then you are in luck. Go home and prepare to card, because you don't have much time until the card will go bad probably. This method is not a very good one, use only if you are desperate.

V. TRW

I will keep this short because this uses more hacking than carding... But one method is to hack the local TRW system and you can get full info on a card with name and number. What you do is find a carbon with partial info some other way (Must be name and number) and check TRW for it, then you will get full info. Personnally, I never hacked TRW on my own although it can be done. Also, you may know some big time hacker through bbsing, have him hack TRW for you and get the info in exchange for carding him something.

VI. Trading info

Another way to get credit card numbers is to just trade information of some sort to someone who has a steady supply of credit cards. Maybe this would be phreaking codes, or dialups, or maybe some bank numbers, or even money I suppose(This would make you a lamer in my book) . There are many people out there who have connections you don't, and some may even give you the numbers and such for free.

VII. VMB's and Carding Subs

This is basically self explanitory. There are many Voice Mail Boxes or VMBs that have cards with full info on them, and they are not that hard to get the number to, just e-mail some people you know, maybe they know of one. Just, once in a while put in a valid card and then all will go well. Also many elite systems have their own carding sub, there will be valid cards on these subs for the taking. Don't be shy, although if the card number is really old don't bother, you are just asking to get caught.

VIII. Connections

Maybe you know someone who can do one of the above methods. Don't be afraid to ask for his help. Maybe this person is a cashier that can get you a steady supply of credit card numbers with names. Then get those to someone who hacks TRW and then you will get the

full info on several cards and be able to take you pick and return the favor to some VMBs you leeched card numbers off of...It all works out very nicely...

♠

THE BAUDY WORLD OF THE BYTE BANDIT: A POSTMODERNIST INTERPRETATION OF THE COMPUTER UNDERGROUND

An earlier version of this paper was presented at the American Society of Criminology annual meetings, Reno (November 9, 1989). Authors are listed in alphabetical order. Address correspondence to Jim Thomas. We are indebted to the numerous anonymous computer underground participants who provided information. Special acknowledgement goes to Hatchet Molly, Jedi, The Mentor, Knight Lightning, and tran King.

ABSTRACT

The criminalization of "deviant acts" transforms social meanings into legal ones. Yet, legal meanings are not necessarily social meanings. The legitimacy of statutory social control generally requires that one accept the realist textual readings of those with the power to interpret and stigmatize behaviors as inappropriate. "Moral crusades" that lead to definitions of criminalized deviance tend to reduce the meanings of polysemic

acts to unidimensional ones that limit understanding of both the nature of the acts and their broader relationship to the culture in which they occur. This has occured with the criminalization of computer phreaking and hacking. In this paper, we examine the computer underground as a cultural, rather than a deviant, phenomenon. Our data reveal the computer underground as an invisible community with a complex and interconnected culture, dependent for survival on information sharing, norms of reciprocity, sophisticated socialization rituals, and an explicit value system. We suggest that the dominant image of the computer underground as one of criminal deviance results in a failure to appreciate cultural meaning. We conclude by arguing that there are characteristics of underground activity that embrace a postmodernist rejection of conventional culture. Hackers are "nothing more than high-tech street gangs" (Federal Prosecutor, Chicago). Transgression is not immoral. Quite to the contrary, it reconciles the law with what it forbids; it is the dialectical game of good and evil (Baudrillard, 1987: 81). There ain't no sin and there ain't no virtue. There's just stuff people do. It's all part of the nice, but that's as far as any man got a right to say (Steinbeck, 1939:31-32).

The criminalization of "deviant acts" transforms and reduces social meanings to legal ones. Legal meanings are not necessarily social meanings. Most deviancy research tends to reproduce conventional social ideology and operative definitions of normality within its concepts and theories. On occasion, these meanings represent a form of "class politics" that protect the power and privilege of one group from the challenge of another: Divorcing moral crusades from status group competition while denying that cultures are linked to social classes has undermined attempts to link lifestyle

politics to group struggles (Beisel, 1990: 45). Once a category of behaviors has become defined by statute as sanctionably deviant, the behaviors so-defined assume a new set of meanings that may obscure ones possessed by those who engage in such behaviors. "Computer deviants" provide one example of a criminalized type of "lifestyle politics."

The proliferation of computer technology has been a accompanied by the growth of a computer underground (CU), often mistakenly labeled "hackers," that is perceived as criminally deviant by the media, law enforcement officials, and researchers. Drawing from ethnographic data, we offer a cultural rather than a criminological analysis of the underground by suggesting that it reflects an attempt to recast, re-appropriate, and reconstruct the power-knowledge relationship that increasingly dominates the ideology and actions of modern society. Our data reveal the computer underground as an invisible community with a complex and interconnected cultural lifestyle, an inchoate anti-authoritarian political consciousness, and dependent on norms of reciprocity, sophisticated socialization rituals, networks of information shaand an explicit value system. We interpret the CU culture as a challenge to and parody of conventional culture, as a playful attempt to reject the seriousness of technocracy, and as an ironic substitution of rational technological control of the present for an anarchic and playful future. Stigmatizing the Computer Underground The computer underground refers to persons engaged in one or more of several activities, including pirating, anarchy, hacking, and phreaking[1]. Because computer underground participants freely share information and often are involved collectively in a single incident, media definitions invoke the generalized metaphors of "conspiracies" and "criminal rings," (e.g., Camper, 1989; Zablit, 1989), "modem macho" evil-doers (Bloombecker, 1988), moral bankruptcy (Schwartz, 1988), "electronic trespassers" (Parker: 1983), "crazy kids dedicated to making mischief" (Sandza, 1984: 17), "electronic vandals" (Bequai: 1987), a new "threat" (Van, 1989), saboteurs

("Computer Sabateur," 1988), secret societies of criminals (WMAQ, 1990), and "high-tech street gangs" ("Hacker, 18," 1989). These images have prompted calls for community and law enforcement vigilance (Conly and McEwen, 1990: 2) and for application of the Racketeer Influenced and Corrupt Organizations (RICO) Act to prosecute and control the "criminals" (Cooley, 1984). These images fail to distinguish underground "hobbyists," who may infringe on legal norms but have no intention of pillaging, from felonious predators, who use technology to loot[2]. Such terminology provides a common stock ofknowledge that formats interpretations of CU activity in ways pre-patterned as requiring social control to protect the common weal (e.g., Altheide, 1985). As Hollinger and Lanza-Kaduce (1988: 119), Kane (1989), and Pfuhl (1987) observed, the stigmatization of hackers has emerged primarily through value-laden nedia

depictions. When in 1990 a Cornell University graduate student inadvertently infected an in ternational computer network by planting a self-reproducing "virus," or "rogue program," the news media followed the story with considerable detail about the dangers of computer abuse (e.g., Allman, 1990; Winter, 1988). Five years earlier, in May of 1983, a group of hackers known as "The 414's" received equal media attention when they broke into the computer system of the Sloan Kettering Cancer research center. Between these dramatic and a typical events, the media have dramatized the dangers of computer renegades, and media anecdotes presented during Congressional legislative debates to curtail "computer abuse" dramatized the "computer hacking problem" (Hollinger and Lanza-Kaduce, 1988: 107). Although the accuracy and objectivity of the evidence has since been challenged (Hollinger and lnza-Kaduce 1988: 105), the media continue to format CU activity by suggesting that any computer-related felony can be attributed to hacking. Additionally, media stories are taken from the accounts of police blotters, security personnel, and apprehended hackers, each of whom have different perspectives and definitions. This creates a self-rein-forcing imagery in which extreme examples and cursively circulated data are discretely adduced to substantiate the claim of criminality by those with a vested interest in creating and maintaining such definitions. For example, Conly and McEwen (1990) list examples of law enforcement jurisdictions in which special units to fight "computer crime," very broadly defined, have been created. These broad definitions serve to expand the scope of authority and resources of the units. Nonetheless, despite criminalization, there is little evidence to support the contention that computer hacking has been sufficiently abusive or pervasive to warrant prosecution (Michalowski and Pfuhl, forth-coming). As an antidote to the conventional meanings of CU activity as simply one of deviance, we shift the social meaning of CU behavior from one of stigma to one of culture creation and meaning. Our work is tentative, in part because of the lack of previous substantive literature and in part because of the complexity of the data, which indicate a multiplicity of subcultures within the CU. This paper examines of two distinct CU subcultures, phreaks and hackers, and challenges the Manichean view that hackers can be understood simply as profaners of a sacred moral and economic order. The Computer Underground and Postmodernism: The computer underground is a culture of persons who call computer bulletin board systems (BBSs, or just "boards"), and share the interests fostered by the BBS. In conceptualizing the computer underground as a distinct culture, we draw from Geertz's (1973: 5) definition of culture as a system of meanings that give significance to shared behaviors that must be interpreted from the perspective of those engaged in them. A culture provides not only the "systems of standards for perceiving, believing, evaluating, and acting" (Goodenough, 1981: 110), but includes the rules and symbols of interpretation and discourse for

partici-pants: Incrude relief, culture can be understood as a set of solutions devised by a group of people to meet specific problems posed by situations they face in common. . . This notion of culture as a living, historical product of group problem solving allows an approach to cultural study that is applicable to any group, be it a society, a neighborhood, a family, a dance band, or an organization and its segments (Van Maanen and Barley, 1985: 33). Creating and maintaining a culture requires continuous individual or group processes of sustaining an identity through the coherence gained by a consistent aesthetic point of view, a moral conception of self, and a lifestyle that expresses those conceptions in one's immediate existence and tastes (Bell, 1976: 36). These behavioral expressions signify a variety of meanings, and as signifiers they reflect a type of code that can be interpreted semiotically, or as a sign system amenable to readings independent of either participants or of those imposed by the super-or-dinate culture: All aspects of culture possess a semiotic value, and the most taken-for-granted phenomena can function as signs: as elements in communication systems governed by semantic rules and codes which are not themselves directly apprehended in experience. These signs are, then, as opaque as the social relations which produce them and which they re-present (Hebdige, 1982: 13). It is this symbolic cultural ethos, by which we mean the style, world view, and mood (Hebdige, 1979), that reflects the postmodernist elements of the CU and separates it from modernism. Modernist culture is characterized especially by rationality, technological enhancement, deference to centralized control, and mass communication. The emergence of computer technology has created dramatic changes in social communication, economic transactions, and information processing and sharing, while simultaneously introducing new forms of surveillance, social control, and intrusions on privacy (Marx, 1988a: 208-211; Marx and Reichman, 1985). This has contributed to a: richly confused and hugely verbal age, energized by a multitude of competing discourses, the very proliferation and plasticity of which increasingly deter mine what we defensively refer to as our reality (New- man, 1985: 15). By Postmodernism we mean a reaction against "cultural moder- nity" and a destruction of the constraints of the present "maximum security society" (Marx, 1988b) that reflect an attempt to gain control of an alternative future. In the CU world, this constitutes a conscious resistance to the domination of but not the fact of technological encroachment into all realms of our social existence. The CU represents a reaction against modernism by offering an ironic response to the primacy of a master technocratic language, the incursion of computers into realms once considered private, the politics of techno-society, and the sanctity of established civil and state authority. Postmodernism is characterized not so much by a single definition as by a number of interrelated characteristics, including, but not limited to:

1. Dissent for dissent's sake (Lyotard, 1988).
2. The collapse of the hierarchical distinction between mass and popular culture (Featherstone, 1988: 203).
3. A stylistic promiscuity favoring eclecticism and the mixing of codes (Featherstone, 1988: 203).
4. Parody, pastiche, irony, playfulness and the celebration of the surface "depthlessness" of culture (Featherstone, 1988: 203).
5. The decline of the originality/genius of the artistic producer and the assumption that art can only be repetitious (Featherstone 1988: 203).
6. The stripping away of social and perceptual coordinates that let one "know where one is" (Latimer, 1984: 121).
7. A search for new ways to make the unpresentable

presentable, and break down the barriers that keep the profane out of everyday life (Denzin, 1988: 471).

8. The introduction of new moves into old games or inventing new games that are evaluated pragmatically rather than from some uniform stand point of "truth" or philosophical discourse (Callinicos, 1985: 86).
9. Emphasis on the visual over the literary (Lash, 1988: 314).
10. Devaluation of formalism and juxtaposition of signifiers taken from the banalities of everyday life (Lash, 1988: 314).
11. Contesting of rationalist and/or didactive views of culture (Lash, 1988: 314).
12. Asking not what a cultural text means, but what it does (Lash, 1988: 314).
13. Operation through the spectator's immersion, the relatively unmediated investment of his/her desire in the cultural object (Lash, 1988: 314).
14. Acknowledgement of the decenteredness of modern life and "plays with the apparent emptiness of modern life as well as the lack of coherence in modern symbol systems" (Manning, 1989: 8).

"Post-Modernism" in its positive form constitutes an intellectual attack upon the atomized, passive and indifferent mass culture which, through the saturation of electronic technology, has reached its zenith in Post-War American (Newman, 1985: 5). It is this style of playful rebellion, irreverent subversion, and juxtaposition of fantasy with high-tech reality that impels us to interpret the computer underground as a postmodernist culture.

Data and Method: Obtaining data from any underground culture requires tact. BBS operators protect the privacy of users and access to elite boards, or at least to their relevant security

levels, virtually always requires completion of a preliminary questionnaire, a screening process, and occasional voice verification. Researchers generally do not themselves violate laws or dominant norms, so they depend on their informants for potentially "dirty information" (Thomas and Marquart, 1988). Our own data are no exception and derive from several sources. First, the bulk of our data come from computer bulletin board systems. BBSs are personal computers (PCs) that have been equipped with a telephone modem and special software that connects users to other PCs by telephone. After "logging in" by supplying a valid user name and password, the user can receive and leave messages to other users of the system. These messages are rarely private and anyone calling the BBS can freely read and respond to them. There is usually the capacity to receive (download) or send (upload) text files ("G-philes") or software programs between the caller and host system. We logged the message section of CU BBSs to compile documentary evidence of the issues deemed important for discussion by participants. Logs are "captured" (recorded using the computer buffer) messages left on the board by users. Calculating the quantity of logged data is difficult because of formatting variance, but we estimate that our logs exceed 10,000 printed pages. The logs cited here are verbatim with the exception of minor editing changes in format and extreme typographical errors. Identifying underground BBSs can be difficult, and to the uninitiated they may appear to be licit chat or shareware boards. For callers with sufficient access, however, there exist back-stage realms in which "cracking" information is exchanged and private text or software files made available. With current technology, establishing a BBS requires little initial skill. Most boards are short-lived and

serve only local or regional callers. Because of the generally poor quality and amateur nature of these systems, we focused on national elite boards. We considered a board "elite" if it met all of the following characteristics: At least one quarter of the users were registered out side the state of the board called; the phone line were exclusively for BBS use and available 24 hours a day; and the information and files, warez were current "state of the field." Elite CU members argue that there are less than ten "truly elite" p/hacker boards nationally. We obtained the names and numbers of BBSs from the first boards we called, and used a snowball technique to supplement the list. We obtained additional numbers from CU periodicals,and, as we became more familiar with t he culture, users also added to the list. Our aggregate data include no less than 300 Bulletin board systems, of which at least 50 attract phreaks and hackers, and voice or on-line interviews with no less than 45 sysops (operators of BBS systems) and other active CU participants. A second data source included open-ended voice and on-line interviews with hackers, phreaks and pirates. The data include no less than 25 face-to-face, 25 telephone, and 60 on-line interviews obtained as we became familiar with our informants. Third, data acquisition included as much participation as legally possible in

CU activities[3]. This served to justify our presence in the culture and provided information about the mundane activity of the CU. Finally, we obtained back and current issues of the primary underground computerized magazines, which are distributed on national BBSs as text files. These contain information relevant to the particular subculture, and included PHRACK, Activist Times Incorporated (ATI), P/Hun, 2600 Magazine, PIRATE, TAP, Al.P.H.A and Legion of Doom (LoD/H). We also draw data from national and international electronic mail (e-mail) systems on which an active information-sharing CU network has developed and spread. Assessing the validity and reliability of data obtained in this manner creates special problems. One is that of sampling. The number of boards, their often ephemeral existence, and the problem of obtaining access makes conventional sampling impossible. We focused on national boards and engaged in theoretical sampling (Glaser and Strauss, 1967: 45-77). We consider our sample representative, and accept Bordieu's observation that: If, following the canon dictated by orthodox methodology, you take a random sample, you mutilate the very object you have set out to construct. If, in a study of the field of lawyers, for instance, you do not draw the President of the Supreme Court, or if, in an inquiry into the French intellectual field of the 1950s, you leave out Jean-Paul Sartre, or Princeton University in a study of American academics, your field is destroyed, insofar as these personas or institutions alone mark a crucial position--there are positions in a field which command the whole structure (Bordieu, interviewed in Wacquant, 1989: 38). We judge our sample of participants adequate for several reasons. First, we presume that the members with whom we have had contact comprise the elite members of the culture, as determined by the nature of the boards they were on, references to them on national boards, the level of expertise displayed in their messages, and their appearance in the "user lists" of elite boards. We consider the BBSs to be "typical exemplars" because of their status in the culture, because of the level of sophistication both of users and of message content, and because of references to these boards as "elite" in CU periodicals.

The computer underground is both a life style and a social network. As a lifestyle, it provides identity and roles, an operational ideology, and guides daily routine. As a social net-work, it functions as a communications channel between persons engaged in one of three basic activities: Hacking, phreaking, and pirating[4]. Each subgroup possesses an explicit style that includes an ethic and "code of honor," cohesive norms,

career paths, and other characteristics that typify a culture (Meyer, 1989a, 1989b;; Meyer and Thomas, 1989). Hebdige (1982: 113-117) used the concept of homology to describe the structural unity that binds participants and provides the "symbolic fit between the values and life-styles of a group" and

how it expresses or reinforces its focal concerns. Homology refers to the affinity and similarities members of a group share that give it the particular cultural identity. These shared alternative values and actions connect CU members to each other and their culture, and create a celebration of "otherness" from the broader culture. Hackers (Tune: "Put Another Nickel in") Put another password in, Bomb it out, and try again, Try to get past logging in, Were hacking, hacking, hacking. Try his first wife's maiden name, This is more than just a game, It's real fun, but just the same It's hacking, hacking, hacking. Sys-call, let's try sys-call. Remember, that great bug from Version 3, Of R S X, It's here! Whoopee! Put another sys-call in, Run those passwords out and then, Dial back up, we're logging on, We're hacking, hacking, hacking. (The Hacker Anthem, by Chesire Catalyst) Hacking broadly refers to attempts to gain access to computers to which one does not possess authorization. The term "hackers" first came into use in the early 1960's when it was applied to a group of pioneering computer aficionados at MIT (Levy, 1984). Through the 1970s, a hacker was viewed as someone obsessed with understanding and mastering computer systems (Levy 1984). But, in the early 1980's, stimulated by the release of the movie "War Games" and the much publicized arrest of a "hacker gang" known as "The 414s", hackers were seen as young whiz-kids capable of breaking into corporate and government computer systems (Landreth 1985:34). The imprecise media definition and the lack of any clear understanding of what it means to be a hacker results in the mis-application of the label to all forms of computer malfeasance. Despite the inter-relationship between phreaks and hackers, the label of "hacker" is generally reserved for those engaged in computer system trespassing. For CU participants, hacking can mean either attempting to gain access to a computer system, or the more refined goals of exploring in, experimenting with, or testing a computer system. In the first connotation, hacking re quires skills to obtain valid user accounts on computer systems that would otherwise be unavailable, and the term connotes the repetitive nature of break-in attempts. Once successful entry is made, the illicit accounts are often shared among associates and described as being "freshly (or newly) hacked." The second connotation refers to someone possessing the knowledge, ability, and desire to fully explore a computer system. The elite hackers, the mere act of gaining entry is not enough to warrant the "hacker" label; there must be a desire to master and skill to use the system after access has been achieved: It's Sunday night, and I'm in my room, deep into a hack. My eyes are on the monitor, and my hands are on the keyboard, but my mind is really on the operating system of a super-minicomputer a thousand miles away - a super-mini with an operating systems that does a good job of tracking users, and that will show my activities in its user logs, unless I can outwit it in the few hours before the Monday morning staff arrives for work.....Eighteen hours ago, I managed to hack a pass-word for the

PDP 11/44. Now, I have only an hour or so left to alter the user logs. If I don't the logs will lead the system operators to my secret account, and the hours of work it took me to get this account will be wasted (Landreth, 1985: 57-58). An elite hacker must experiment with command structures and explore the many

files available in order to understand and effectively use the system. This is sometimes called "hacking around" or simply "hacking a system". This distinction is necessary because not all trespassers are necessarily skilled at hacking out passwords, and not all hackers retain interest in a system once the challenge of gaining entry has been surmounted. Further, passwords and accounts are often traded, allowing even an unskilled intruder to erroneously claim the title of "hacker." Our data indicate that, contrary to their media image, hackers avoid deliberately destroying data or otherwise damaging the system. Doing so would conflict with their instrumental goal of blending in with the average user to conceal their presence and prevent the deletion of the account. After spending what may be a substantial amount of time obtaining a high access account, the hacker places a high priority on not being discovered using it, and hackers share considerable contempt for media stories that portray them as "criminals." The leading CU periodicals (e.g., PHRACK, PIRATE) and several CU "home boards" reprint and disseminate media stories, adding ironic commentary. The perception of media distortion also provides grist for message sections: A1: I myself hate newspaper reporters who do stories on hackers, piraters, phreaks, etc...because they always make us sound like these incred. %sic% smart people (which isn't too bad) who are the biggest threat to to-days community. Shit...the BEST hackers/phreaks/etc will tell you that they only do it to gain information on those systems, etc...(Freedom - That's what they call it...right?) (grin) A2: Good point...never met a "real p/h type yet who was into ripping off. To rip of a line from the Steve Good-man song (loosely), the game's the thing. Even those who allegedly fly the jolly rodger %pirates%, the true ones, don't do it for the rip-off, but, like monopoly, to see if they can get Boardwalk and Park Place without losing any railroads. Fun of the latter is to start on a board with a single good game or util %software utility% and see what it can be turned into, so I'm told. Fuck the press (DS message log, 1989). One elite hacker, a member of a loose-knit organization recently in the national news when some participants were indicted for hacking, responded to media distortions of the group by issueing an underground press release: My name is %deleted%, but to the computer world, I am %deleted%. I have been a member of the group known as Legion of Doom since its creation, and admittedly I have not been the most legitimate computer user around, but when people start hinting at my supposed Communist-backed actions, and say that I am involved in a world- wide conspiracy to destroy the nation's computer and/or 911 network, I have to speak up and hope that people will take what I have to say seriously. . . . People just can't seem to grasp

the fact that a group of 20 year old kids just might know a little more than they do, and rather than make good use of us, they would rather just lock us away and keep on letting things pass by them. I've said this before, you can't stop burglars from robbing you when you leave the doors unlocked and merely bash them in the head with baseball bats when they walk in. You need to lock the door. But when you leave the doors open, but lock up the people who can close them for you another burglar will just walk right in ("EB," 1990). Although skirting the law, hackers possess an explicit ethic and their primary goal is knowledge acquisition. Levy (1984: 26-36) identifies six "planks" of the original hacker ethic, and these continue to guide modern hackers: 1. First, access to computers should be unlimited and total: "Always yield to the Hands-On Imperative!" 2. Second, all information should be free. 3. Third, mistrust authority and promote decentralization. 4. Fourth, hackers should be judged by their prowess as hackers rather than by formal organizational or other irrelevant criteria. 5. Fifth, one can create art and beauty on a computer. 6. Finally, computers can change lives for the better. PHRACK, recognized as the

"official" p/hacker newsletter, expanded on this creed with a rationale that can be summarized in three principles ("Doctor Crash," 1986). First, hackers reject the notion that "businesses" are the only groups entitled to access and use of modern technology. Second, hacking is a major Weapon in the fight against encroaching computer technology. Finally, the high cost of equipment is beyond the means of most hackers, which results in the perception that hacking and phreaking are the only recourse to spreading computer literacy to the masses: Hacking. It is a full time hobby, taking countless hours per week to learn, experiment, and execute the art of penetrating multi-user computers: Why do hackers spend a good portion of their time hacking? Some might say it is scientific curiosity, others that it is for mental stimulation. But the true roots of hacker motives run much deeper than that. In this file I will describe the underlying motives of the aware hackers, make known the connections between Hacking, Phreaking, Carding, & Anarchy, and make known the "techno-revolution" which is laying seeds in the mind of every hacker. . . .If you need a tutorial on how to perform any of the above stated methods %of hacking%, please read a %PHRACK% file on it. And whatever you do, continue the fight. Whether you know it or not, if you are a hacker, you are a revolutionary. Don't worry, you're on the right side ("Doctor Crash," 1986). Computer software, such as auto-dialers popularized in the film War Games, provides a means for inexperienced hackers to search out other computers. Auto-dialers randomly dial numbers and save the "hits" for manual testing later. Some users self-i-dentify has hackers simply on the basis of successfully collecting computer numbers or passwords, but these users are considered lamerz," because they do not possess sufficient knowledge to obtain access or move about in the system once access is obtained. Lamerz are

readily identified by their message content: Sub ->numbers From -> (#538) To ->all Date ->02/21/xx 06:10:00 PM: Does anyone know any numbers for hotels, schools, businesses, etc..and passwords if you do please leave a bulletin with the number and the password and/or logon id. Sub ->phun From -> (#138) To ->all Date ->02/22/xx 12:21:00 AM Anyone out there got some good 800 dial up that are fairly safe to hack? If so could ya leave me em in e-mail or post em with the formats.....any help would%be apreciated.....
thanx

Although hackers freely acknowledge that their activities may be occasionally illegal, considerable emphasis is placed on limiting violations only to those required to obtain access and learn a system, and they display hostility toward those who transgress beyond beyond these limits. Most experienced CU members are suspicious of young novices who are often entranced with what they perceive to be the "romance" of hacking. Elite hackers complain continuously that novices are at an increased risk of apprehension and also can "trash" accounts on which experienced hackers have gained and hidden their access. Nonetheless, experienced hackers take pride in their ethic of mentoring promising newcomers, both through their BBSs and newsletters: As %my% reputation grew, answering such requests [from novice hackers wanting help] became a matter of pride. No matter how difficult the question happened to be, I would sit at the terminal for five, ten, twenty hours at a time, until I had the answer (Landreth, 1985: 16). The nation's top elite p/hacker board was particularly nurturing of promising novices before it voluntarily closed in early 1990, and its sysop's handle means "teacher." PHRACK, begun in 1985, normally contained 10-12 educational articles (or "philes"), most of which provided explicit sophisticated technical information about computer networks and telecommunications systems[5]. Boundary socialization occurs in message bases and newsletters that either discourage such activity or provide guidelines for concealing access once obtained: Welcome to the world of hacking! We, the

people who live outside of the normal rules, and have been scorned and even arrested by those from the 'civilized world', are becoming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgements here) can do nowadays, thus causing anti-hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the 'higher' authorities who monitor the system. This article is intended to tell you about some things not to do, even before you get on the system. We will tell you about the new wave of front end security devices that are beginning to be used on computers. We will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble. (p/hacker newsletter, 1987). Elite hacking requires highly sophisticated technical skills to enter

the maze of protective barriers, recognize the computer type, and move about at the highest system levels. As a consequence, information sharing becomes the sine qua non of the hacker culture. "Main message" sections are generally open to all users, but only general information, gossip, and casual commentary is posted. Elite users, those with higher security privileges and access to the "backstage" regions, share technical information and problems, of which the following is typical:

> 89Mar11
> From ***** ** * ***>
> Help! Anyone familiar with a system that responds:
> A2: SELECT : DISPLAY:
> 1=TRUNK,2=SXS;INPUT:3=TRUNK,4=SXS,5=DELETE;7=MSG <and then it gives you a prompt> If you chose 1... ENTER OLD#,(R=RETURN)
> At this point I know you can enter 7 digits, the 8th ill give you an INVALID ENTRY type message. Some numbers don't work however. (1,2,7,8 I know will) Anybody?
> 89Mar10
> From *********>
> I was hacking around on telenet (415 area code) and got a few things that I am stuck-o on if ya can help, I'd be greatly happy. First of all, I got one that is called RCC PALO ALTO and I can't figure it out. Second (and this looks pretty fun) is the ESPRIT COMMAIL and I know that a user name is SYSTEM because it asked for a password on ONLY that account (pretty obvious eh?) a few primnet and geonet nodes and a bunch of TELENET ASYYNC to 3270 SERVICE. It asks for TERMINAL TYPE, my LU NUMBER and on numbers higher than 0 and lower that 22 it asks for a password. Is it an outdial? What are some common passwords? then I got a sushi-primnet system. And a dELUT system. And at 206174 there is JUST a : prompt. help! (P/h message log, 1988).

Rebelliousness also permeates the hacker culture and is reflected in actions, messages, and symbolic identities. Like other CU participants, hackers employ handles (aliases) intended to display an aspect of one's personality and interests, and a handle can often reveal whether its owner is a "lamer" (an incompetent) or sophisticated. Hackers take pride in their assumed names, and one of the greatest taboos is to use the handle of an other or to use multiple handles. Handles are borrowed liberally from the anti-heros of science fiction, adventure fantasy, and heavy metal rock lyrics, particularly among younger users, and from word plays on technology, nihilism, and violence. The CU handle reflects a stylistic identity heavily influenced by metaphors reflecting color (especially red and black), supernatural power (e.g., "Ultimate

Warrior, "Dragon Lord"), and chaos ("Death Stalker," "Black Avenger"), or ironic twists on technology, fantasy, or symbols of mass culture (e.g., Epeios, Phelix the Hack, Ellis Dea, Rambo Pacifist, Hitch Hacker).

This anti-establishment ethos also provides an ideological unity for collective action. Hackers have been known to use their collective skills in retaliation for acts against the culture that the perceive as unfair by, for example, changing credit data or "revoking" driver's licenses (Sandza, 1984; "Yes, you Sound very Sexy," 1989). Following a bust of a national hacker group, the message section of the "home board" contained a lively debate on the desireability of a retaliatory response, and the moderates prevailed. Influenced especially by such science fantasy as William Gibson's Neuromancer (1984), John Brunner's The Shockwave Rider (1975), and cyber-punk, which is a fusion of elements of electronic communication technology and the "punk" subculture, the hacker ethic promotes resistance to the very forms that create it. Suggestive of Frazer's (1922) The Golden Bough, power is challenged and supplanted by rituals combining both destruction and rejuvenation. From this emerges a shared ethos of opposition against perceived Orwellian domination by an information-controlling elite:(Hackers will) always be necessary, especially in the technological oppression of the future. Just imagine an information system that systematically filters out certain obscene words. Then it will move on to phrases, and then entire ideas will be replaced by computers! Anyway, there will always be people tripping out on paper and trying to keep it to themselves, and it's up to us to at least loosen their grasp (P.A. Message Log 1988).

Another hacker summarized the near-anarchist ethic characterized the CU style: Lookit, we're here as criminal hobbyists, peeping toms, and looters. I am in it for the fun. Not providing the public what it has a right to know, or keeping big brother in check. I couldn't care less. I am sick of the old journalistic hackers nonsense about or (oops! OUR) computerized ego...I make no attempt to justify what I am doing. Because it doesn't matter. As long as we live in this goddamn welfare state I might as well have some fun taking what isn't mine, and I am better off than those welfare-assholes who justify their stealing. At least I am smart enough to know that the free lunch can't go on forever (U.U. message log 1988).

In sum, the hacker style reflects well-defined goals, communication networks, values, and an ethos of resistance to authority. Because hacking requires a broader range of knowledge than does phreaking, and because such knowledge can be acquired only through experience, hackers tend to be both older and more knowledgeable than phreaks. In addition, despite some overlap, the goals of the two are somewhat dissimilar. As a consequence, each group constitutes a separate analytic

category. Phreaks. Running numbers is not only fun; it's a moral imperative! (Phreak credo). Phreaking broadly refers to the practice of using either technology or telephone credit card numbers (called "codez") to avoid long distance charges. Phreaking attained public visibilily with the revelation of the exploits of John "Cap'n Crunch" Draper, the "father of phreaking" (Rosenbaum, 1971). Although phreaking and hacking each require different skills, phreaks and hackers tend to associate on same boards. Unlike hackers, who attempt to master a computer system and its command and security structure, phreaks struggle to master telecom (tele-communications) technology: The phone system is the most interesting, fascinating thing that I know of. There is

so much to know. Even phreaks have their own areas of knowledge. There is so much to know that one phreak could know something fairly important and the next phreak not. The next phreak might know 10 things that the first phreak doesn't though. It all depends upon where and how they get their info. I myself would like to work for the telco, doing something interesting, like programming a switch. Something that isn't slave labor bullshit. Something that you enjoy, but have to take risks in order to participate unless you are lucky enough to work for Bell/AT&T/any telco. To have legal access to telco things, manuals, etc. would be great (message log, 1988). Early phreaking methods involved electro-mechanical devices that generated key tones or altered phone line voltages to trick the mechanical switches of the phone company into connecting calls without charging, but the advent of computerized telephone-switching systems largely made these devices obsolete. In order to continue their practice, phreaks have had to learn hacking skills in order to obtain access to telephone company computers and software.

Access to telecom information takes several forms, and the possesion of numbers for "loops" and "bridges," while lying in a grey area of law, further enhances the reputation and status of a phreak. P/hackers can utilize "loop lines" to limit the number of eavesdroppers on their conversations. Unlike bridges, which connect an unlimited number of callers simultaneously, loops are limited to just two people at a time[6]. A "bridge" is a technical name for what is commonly known as a "chat line" or "conference system." Bridges are familiar to the public as the pay-per-minute group conversation systems advertised on late night television. Many bridge systems are owned by large corporations that maintain them for business use during the day. While the numbers to these systems are not public knowledge, many of them have been discovered by phreaks who then utilize the systems at night. Phreaks are skilled at arranging for a temporary, private bridge to be created via ATT's conference calling facilities. This provides a helpful information sharing technique among a self-selected group of phreak/hackers: Bridges can be extremely useful means of distributing information as long as the %phone% number is not known, and you don't have a

bunch of children online testing out their DTMF. The last great discussion I participated with over a bridge occurred about 2 months ago on an AT&T Quorum where all we did was engineer 3/way %calls% and restrict ourselves to purely technical information. We could have convinced the Quorum operators that we were AT&T technicians had the need occurred. Don't let the kids ruin all the fun and convenience of bridges. Lameness is one thing, practicality is an other (DC, message log, 1988). Phreaks recognize their precarious legal position, but see no other way to "play the game:" Phreaking involves having the dedication to commit yourself to learning as much about the phone system/ network as possible. Since most of this information is not made public, phreaks have to resort to legally questionable means to obtain the knowledge they want (TP2, message log, 1988). Little sympathy exists among experienced phreaks for "teleco ripoff." "Carding," or the use of fraudulent credit cards, is anathema to phreaks, and not only violates the phreaking ethic, but is simply not the goal of phreaking: Credit card fraud truly gives hacking a bad name. Snooping around a VAX is just electronic voyeurism. carding a new modem is just flat out blue-collar-crime. It's just as bad as breaking into a house or kicking a puppy! %This phreak% does everything he can (even up to turning off a number) to get credit information taken off a BBS. %This phreak% also tries to remove codes from BBSes. He doesn't see code abuse in the same light as credit card fraud, (although the law does), but posted codes are the quickest way to get your board busted, and your computer confiscated. People should just find a local outdial to

wherever they want to call and use that. If you only make local calls from an outdial, it will never die, you will keep out of trouble, and everyone will be happy (PHRACK, 3(28): Phile 2). Experienced phreaks become easily angered at novices and "lamerz" who engage in fraud or are interested only in "leeching" (obtaining something for nothing):

Sub ->Carding
From ->JB (#208)
To ->ALL
Date ->02/10/xx 02:22:00 PM

what do you people think about using a parents card number for carding? For instance, if I had a friend order and receive via next day air on my parents card, and receive it at my parents house while we were on vacation. Do you think that would work? Cuz then, all that we have to do is to leave the note, and have the bud pick up the packages, and when the bill came for over $1500, then we just say... 'Fuck you! We were on vacation! Look at our airline tickets!' I hope it does... Its such a great plan!

Sub ->Reply to: Carding
From -> (xxx)
To -> X
Date ->02/11xx 03: 16:00 AM

NO IT'S NOT A GREAT IDEA! WHERE'S YOUR SENSE OF RESPONSIBILITY TO YOUR FAMILY? ARE THEY ALL IN AGREEMENT WITH YOU? WOULD YOU WANT ANYONE TO USE YOUR PRIVATE STUFF IN ILLEGAL (AND IMMORAL) ACTIVITIES WITHOUT YOUR KNOWLEDGE? DIDJA EVER HEAR ABOUT TRUST BETWEEN FAMILY MEMBERS? IF YOU'RE GOING TO BE A THIEF (AND THAT'S NOT NEAT LIKE JAMES BOND IN THE MOVIES), TAKE THE RISKS ONLY UPON YOURSELF!

Sub ->Carding
From -> (#208)
To -> (#47)
Date ->02/12/xx 11: 18:00 AM

Why not? We have a law that says that we have the right to refuse payment to credit cards if there are fraudulent charges. All we do and it is settled.... what is so bad about it? I'm going for it!

Sub ->Reply to: Carding
From -> (xxx)
To ->J.B.
Date ->02/13/xx 02:08:00 AM

APPARENTLY YOU MISSED THE MAIN POINTS I TRIED TO MAKE TO YOU . . YOU'RE A THIEF AND A LIAR, AND ARE BETRAYING THE TRUST OF YOUR FAMILY AS WELL AS INVOLVING THEM IN YOUR RISK WITHOUT THEIR KNOWLEDGE. THAT MEANS YOU ARE A FAIRLY SCUMMY INDIVIDUAL IF YOU GO THROUGH WITH IT! NOW AS TO YOUR "DEFENCE" ABOUT $50 MAXIMUMS AND ERRONEOUS BILLINGS.. LAW MAKES A CLEAR DISTINCTION ABOUT THEFT BY FRAUD (OF WHICH YOU WOULD BE GUILTY). AND IN A LARGER SENSE, YOUR THEFT JUST MAKES IT MORE COSTLY FOR YOU YOU AND EVERYBODY ELSE TO GET CREDIT, AND DO BUSINESS WITH CREDIT CARDS. YOU'RE GOING TO DO WHATEVER YOU DO ANYWAY.....DON'T LOOK FOR ANY APPROVAL IN THIS DIRECTION.

Ironically, experienced phreaks are not only offended by such disregard of law, but also feel that "rip-off artists" have no information to share and only increase the risk for the "tech-no-junkies." Message boards reflect hostility toward apprehended "lamerz" with such comments as "I hope they burn him," or "the lamer probably narked %turned informant% to the pheds %law enforcement agents%." Experienced phreaks also post continual reminders that some actions, because of their illegality, are simply unacceptable: It should be pointed out however, that

should any of you crack any WATS EXTENDER access codes and attempt to use them, you are guilty of Theft of communications services from the company who owns it, and Bell is very willing and able to help nail you! WATS EXTENDERS can get you in every bit as much trouble as a Blue Box should you be caught. Ex-phreaks, especially those who are no longer defined by law as juveniles, often attempt to caution younger phreaks from pursuing phreaking: ZA1: One thing to consider, also, is that the phone co. knows where the junction box is for all of the lines that you are messing with

and if they get enough complaints about the bills, they may start to check things out (I hope your work is neat). I would guess that the odds are probably against this from happening though, because when each of the people call to complain, they'll probably get a different person from the others. This means that someone at Ma Bell has to notice that all of the complaints are coming from the same area...I don't think anybody there really cares that much about their job to really start noticing things like that. anyway, enjoy!!! My guess is that you're under-age. Anyway, so if they catch you, they won't do anything to you anyway. ZB1: Yeah I am a minor (17 years old) I just hope that they don't cause I would like to not have a criminal or juvenile record when I apply to college. Also if they do come as I said in the other message if there are no wires they can't prove shit. Also as I said I only hook up after 6 p.m. The phone company doesn't service people after 6 p.m. Just recently (today) I hooked up to an empty line. No wires were leading from the two plugs to somebody house but I got a dial tone. How great. Don't have to worry about billing somebody else. But I still have to disconnect cause the phone bills should be coming to the other people pretty soon. HEHEHEHE ZX1: Be cool on that, especially if you're calling other boards. Easiest way for telecom security to catch you is match the number called to the time called, call the board, look at users log or messages for hints of identity, then work from there. If you do it too much to a pirate board, they can (and have successfully) pressured the sysop to reveal the identity under threat of prosecution. They may or may not be able to always trace it back, but remember: Yesterday's phreaks are today's telecom security folk. AND: IT'S NOT COOL TO PHREAK TO A PIRATE BOARD...draws attention to that board and screws it up for everybody. So, be cool phreaking....there's safer ways. ZC2: Be cool, Wormburger. They can use all sorts of stuff for evidence. Here's what they'd do in Ill. If they suspected you, they'd flag the phone lines, send somebody out during the time you're on (or they suspect you're on) and nail you. Don't want to squelch a budding phreak, but you're really taking an unnecessary chance. Most of us have been doing stuff for some time, and just don't want to see you get nailed for something. There's some good boards with tips on how to phreak, and if you want the numbers, let me know. We've survived to warn you because we know the dangers. If you don't know what ESS is, best do some quick research (P/h message log, 1988).

In sum, the attraction of phreaking and its attendant life-style appear to center on three fundamental characteristics: The quest for knowledge, the belief in a higher ideological purpose of opposition to potentially dangerous technological control, and the enjoyment of risk-taking. In a sense, CU participants consciously create dissonance as a means of creating social meaning in what is perceived as an increasingly meaningless world (Milo-vanovic and Thomas, 1989). Together, phreaks and hackers have created an

overlapping culture that, whatever the legality, is seen by participants as a legitimate enterprise in the new "tech-no-society."

Conclusion: The transition to an information-oriented society dependent on computer technology brings with it new symbolic metaphors and behaviors. Baudrillard (1987: 15) observed that our private sphere now ceases to be the stage where the drama of subjects at odds with their objects and with their image is played out, and we no longer exist as playwrites or actors, but as terminals of multiple networks. The public space of the social arena is reduced to the private space of the computer desk, which in turn creates a new semi-public, but restricted, public realm to which dissonance seekers retreat. To participate in the computer underground is to engage in what Baudrillard (1987: 15) describes as private telematics, in which individuals, to extend Baudrillard's fantasy metaphor, are transported from their mundane computer system to the controls of a hypothetical machine, isolated in a position of perfect sovereignty, at an infinite distance from the original universe. There, identity is created through symbolic strategies and collective beliefs (Bordieu, cited in Wacquant, 1989: 35). We have argued that the symbolic identity of the computer underground creates a rich and diverse culture comprised of justifications, highly specialized skills, information-sharing net-works, norms, status hierarchies, language, and unifying symbolic meanings. The stylistic elements of CU identity and activity serve what Denzin (1988: 471) sees as the primary characteristic of postmodern behavior, which is to make fun of the past while keeping it alive and the search for new ways to present the unpresentable in order to break down the barriers that keep theprofane out of the everyday.

The risks entailed by acting on the fringes of legality and substituting definitions of acceptable behavior with their own, the playful parodying of mass culture, and the challenge to authority constitute an exploration of the limits of techno-culture hile resisting the legal meanings that would control such actions. The celebration of anti-heros, re-enacted through forays into the world of computer programs and software, reflects the stylistic promiscuity, eclecticism and code-mixing that typifies the postmodern experience (Featherstone, 1988: 202). Rather than attempt to fit within modern culture and adapt to values and definitions imposed on them, CU participants mediate it by mixing art, science, and resistance to create a culture with an alternative meaning both to the dominant one and to those that observers would impose on them and on their enterprise. Pfuhl (1987) cogently argued that criminalization of computer abuse tends to polarize definitions of behavior. As a conseuence, To view the CU as simply another form of deviance, or as little more than "high-tech street gangs" obscures the ironic, mythic, and subversive element, the Nieztschean "will to power," reflecctd in

the attempt to master technology while challenging those forces that control it. The "new society" spawned by computer technology is in its infancy, and, as Sennet (1970: xvii) observed, the passage of societies through adolescence to maturity requires acceptance of disorder and painful dislocation.

Instead of embracing the dominant culture, the CU has created an irreducible cultural alternative, one that cannot be understood without locating its place within the dialectic of social change. Especially in counter-cultures, as Hebdige (1983: 3) observes, "objects are made to mean and mean again," often
ending: in the construction of a style, in a gesture of defiance or contempt, in a smile or a sneer. It signals a Refusal. I would like to think that this Reusal is worth making, that these gestures have a meaning, that the smiles and the sneers have some subversive value. . . (Hebdige, 1982: 3).

Footnotes
[1] Participants in the computer underground engage in considerable

word play that includes juxtaposition of letters. For example, commonly used words beginning with "f" are customarily spelled with a "ph." The CU spelling conventions are retained throughout this paper.

[2] Conly and McEwen (1990: 3) classify "software piracy" in the same category as theft of computers and trade secrets, and grossly confuse both the concept and definition of computer crime by conflating any illicit activity involving computers under a definition so broad that embezzlement and bulletin boards all fall within it. However, the label of "computer criminal" should be reserved for those who manipulate computerized records in order to defraud or damage, a point implied by Bequai (1978: 4) and Parker (1983: 106).

[3] One author has been active in the computer underground since 1984 and participated in Summercon-88 in St. Louis, a national conference of elite hackers. The other began researching p/hackers and pirates in 1988. Both authors have had sysop experience with national CU boards. As do virtually all CU participants, we used pseudonyms but, as we became more fully immersed in the culture, our true identities were sometimes revealed.

[4] Although we consider software pirates an integral part of the computer underground, we have excluded them from this analysis both for parsimony and because their actions are sufficiently different to warrant separate analysis (Thomas and Meyer, 1990). We also have excluded anarchist boards, which tend to be utilized by teenagers who use BBSs to exchange information relating to social disruption, such as making homemade explosives, sabotaging equipment, and other less dramatic pranks.

These boards are largely symbolic, and despite the name, are devoid of political intent. However, our data suggest that many hackers began their careers because of the anarchist influence.

[5] In January, 1990, the co-editor of the magazine was indicted for allegedly "transporting" stolen property across state lines. According to the Secret Service agent in charge of the case in Atlanta (personal communication), theoffender was apprehended for receiving copies of E911 ("enhanced" 911 emergency system) documents by electronic mail, but added that there was no evidence that those involved were motivated by, or received, material gain.

[6] "Loop lines" are telephone company test lines installed for two separate telephone numbers that connect only to each other. Each end has a separate phone number, and when each person calls one end, they are connected to each other automatically. A loop consists of "Dual Tone Multi-Frequency," which is the touch tone sounds used to dial phone numbers. These test lines are discovered by phreaks and hackers by programming their home computer to dial numbers at random and "listen" for the distinctive tone that an answering loop makes, by asking sympathetic telephone company employees, or through inormation contained on internal company computers.

Introduction to PBXs by < Grim Reaper >

his file is a personal continuation of the PBX entry in the MCI telecommunications Glossary. A telephone exchange serving an individual organization and having connections to a public telephone exchange is called a Private Branch Exchange (PBX). The PBX performs a switching function by connecting any extension in the private organization to an outside line. A PBX is actually a private switch that connects a group of telephones within an individual organization. Calls placed outside this individual group are connected to a telephone company's central office switch through trunks. A PBX may be operated by an attendant from the private organization or the switching system may be done automatically. Other terms that are commonly used interchangeably with PBX are: Private Automatic Branch Exchange (PABX), Private Automatic Exchange (PAX), and Computerized Branch Exchange (CBX). Although these terms were originally used to identify specific switch structures, today they are often used as synonyms.

PBXs can use any of three basic switching methods: step-by-step (SxS), Cross-bar (X-bar), and computer controlled, to perform the basic function of switching. However, in addition to detecting calls and establishing a transmission link between two telephones, PBXs can do much more.

The common control, often called a central processing unit (CPU), controls the switching matrix that connects the stat ons and trunks. The switching matrix of a PBX performs the same job as does an operator at a manual switchboard or a common control central office switch. The CPU, however, gets its instructions from the "stored program", which contains directions for activities, such as detecting calls, sending them over the best available route, and recording billing information. These computerized electronic switches are used to perform routine, as well as unique, functions that simply weren't practical or even possible with electromechanical switches.

Just as in the public switched network, PBX switches make connection between instruments, or "key telephone sets". We're all familiar with key telephone sets, whether we know them by name or not. They're the business telephones that have six push-button keys lined up below the dial--a red button marked "hold" and five buttons or lines with flashing lights.

Systems with PBXs and key sets have a great deal of flexability in planning for their needs because they can set up their codes to accomplish the functions needed in their particular situations. In fact, the PBX can be programmed so that each individual extension within a system can take advantage of features applicable to its own business needs.

Some of the features that are availiable with PBXs and key systems are: call transfer, which allows internal or external calls to be transferred from one telephone to any other phone in the system; automatic push-button signaling, which indicates the status of all phones in the system with display lights and buttons; one-way voice paging, which can be answered by dialing the operator from the nearest telephone in the system; camp-on, in which a call made to a busy phone automatically waits until the line is idle; and internal and external conference capabilities, which enables outside callers to conference with several inside users.

Some features automatically handle incoming telephone calls. Automatic call waiting not only holds calls made to a busy extension until the extension is free, but also signals the person being called that a call is waiting and informs the caller that he is on hold. Automatic call forwarding will send calls to employees who are temporarily in locations other than their offices, provided they "inform" the PBX where they can be found. Automatic call distribution automatically send an incoming call to the first extension that's not busy--a useful feature for situations in which any one of a group of persons in the organization can adequately respond to incoming calls. Another example is automatic call back, which allows a caller who reaches a busy line to ask the PBX to return his or her call when the line is free.

Still other features provide services such as night telelphone answering, telephone traffic monitoring, and network or hot-line connection. These examples are but a sample from the features possible with computerized PBXs. This is a very brief description of how to use and what to expect on a PBX.

Basically, you call the PBX and you will have to enter a code that can be anywhere from 4 to 6 digits (Note: some PBXs do not require codes). Then you will hear a dial tone. From here you would under normal circumstances dial: 9 + 1 (or 0) + NPA-PRE-SUFF, for long distance dialing or dial 8 for local
dialing.

The most common use of the PBX is to call Alliance Teleconferencing, a teleconference service offered by AT&T. To do this dial: 0700-456-1000,1002,1003,2000,2001,2002.

Note: PBX codes are usually very simple and usually 4 digits.
EX: 0000, 1111, 1234, etc

Introduction To Phreaking by Cat-Trax

[Definitions]

Phreak ["free"k] Verb-1. The act of "Phreaking" 2. The act of

making telephone calls without paying money [Slang]

Phreaker ["free"-k-er] Noun-1. One who engages in the act of "Phreaking"
2. One who makes telephone calls without paying money [Slang]

[Introduction]

Phreaking is a method used by most intelligent people {most often those who use a computer and a Modulator-Demodulator (MoDem)}. If you happen to resemble the major mass of people who do not have the income to afford large phone bills then phreaking is for you. If you live in an area with an Electronic Switching System [ESS] then phreaking is something which should be done in moderate amounts.

[Switching Systems]

Three types of switching systems are present in the United States today:

[1] Step by Step
[2] Crossbar
[3] ESS {Electronic Switching System}

<] Step by Step [>

First switching system used in America, adopted in 1918 and until 1978 Bell had over 53% of all exchanges using Step by Step [SxS]. A long, and confusing train of switches is used for SxS switching.

[> Disadvantages <]
[A] The switch train may become jammed : Blocking call.
[B] No DTMF [Dual-Tone Multi-Frequency]["Touch-tone"].
[C] Much maintanance and much electricity.
[D] Everything is hardwired

+> Identification <+
[A] No pulsing digits ater dialing or DTMF.
[B] Phone Company sounds like many typewriters.
[C] No: Speed calling, Call forwarding, and other services.
[D] Pay-phone wants money first before dial-tone.

<] Crossbar [>

Crossbar has been Bell's primary switcher after 1960. Three types of Crossbar switching exist: Number 1 Crossbar [1XB], Number 4 Crossbar [4XB], and Number 5 Crossbar [5XB]. A switching matrix is used for all the phones in an area. When someone calls, the route is determined and is met up with the othr phone. The matrix is set-up in horizontal and vertical paths. There are no definite distinguishing features of Crossbar switching.

<] ESS [>

You probably were hoping I wouldn't talk about this nightmare, if you did you will know why everyone doesn't want to be reminded about Bell's holocaust on America. With ESS Bell knows: every digwho make excessive calls to WATS numbers [Wide Area Telephone Service][1-800 numbers] or directory assistance. This deadly trap is called "800 Exceptional Calling Report." ESS can be programmed to print logs of who called certain numbers. Electronic Switching

System makes the job of the FBI, Bell Security {The Gestapo in phreakin' tongue}, NSA, and other organizations which like to invade our privacy, extremely easy! Tracing is done in microseconds, and the results are printed out on the monitor of a Gestapo officer. ESS can also pick up
foreign tones on the line, like 2600 Hz. {used in blue boxes, discussed later}. Bell claims that the entire country will be plagued by ESS by the 1990's!

+> Identification <+

[A] Dialing 911 for emergencies.
[B] Dial-tone first for pay-phones.
[C] Calling services, like: Call forwarding, Speed dialing, Call waiting.
[D] ANI [Automatic Number Identification] for long-distance calls.

[[[Note]]] Of the above identifications of the three switching systems, do not solely rely on these descriptions, the best way to find out is to [no!] call your local telephone company.

[Long-Distance Services]

To attempt to help the community {and for private business} companies developed ways to lessen the costs of long-distance calling charges. The companies own their own switching systems and use extenders for callers to call. The way extenders operate:

1] Customer calls service
2] He/she hears a low tone which sounds like a dial-tone
3] She/He either dials the access code then the phone number, or dials the phone number then the access code
4] Is connected to whatever he/she calls.

Aside from Ma Bells collection, the customer recieves a bill for calls made with his/her long-distance company {a supposedly cheaper bill than Ma Bell's}. Thought: Hey, I could randomly pick access codes and use them to call whatever area the company services! Righto, that's what basic phreaking is! A wise idea, though, is to have many access codes and many service numbers to rotate throughout your average life as a phreaker. To aid in your quest to beat the system I have provided many 1-800 numbers which anyone can call, aside from local numbers, such as Sprint, or MCI. The reason for providing you with WATS numbers is because all of us aren't in a big city where Sprint or MCI even exist, this way everyone can pheak! A way to find more access codes is by using your old modem. Yes, your modem can imitate
DTMF tones!

{>Procedure: 1) dial 1-800 + service number
2) dial access code->area code->phone number, or
3) dial area code->phone number->access code

::\/
-=+>Cat-Trax' list of WATS [1-800] numbers:<+=-

::

Number	Code Length	Number	Code Length	Number	Code
127-6754	6	245-4890	4	327-6713	4
243-7650	6	328-7112	4	654-8494	6
327-9895	7	327-9136	4	227-3414	4

682-4000	6	343-1844	4	858-9000	3
462-6471	5	322-1415	6	521-1674	4
527-3511	8	321-0327	4	321-0845	6
843-0698	9	221-8190	4	543-7168	8
521-8400	8	327-2731	6	252-5879	8
345-0008	7	245-7508	5	526-5305	8
323-3027	6	242-1122	?	621-1506	?
621-4611	?	325-3075	?	336-6000	?
221-1950	?	323-8126	?	325-7222	6

[[[Note]]] remember to dial 1-800-above number, also remember to rotate numbers and access codes.

[Colored Boxes]

A more shrewd, technological, safer {without ESS} way to phreak is with a piece of hardware known as a _____ Box. Boxes are many different colors {I don't know ALL the colors because it seems like every time I turn around there's some new color out!}. Colors I have heard of: Blue, Black, Red, White, Silver, Clear, and MANY, MANY more... Plans for making these boxes can be obtained by calling different boards [BBS's], AE lines, or whatever. But!, if you have an Apple Cat modem then do I have good news for ->you<-!! The Apple Cat modem can emulate the frequencies {usually 2600 Hz.} made by _____ Boxes with the help of a handy little program called "Cat's Meow!"

::Warning!:: Phreak at your own risk! Stiff laws are starting to pop-up now days. But, if you're careful then don't worry! I haven't been busted yet! Heck [Hack!], what would life be without risks?

SOME NOTES ON LINE NOISE by Captain KIdd

Well since that's my field let me elucidate abit.... Most of what you refer to as line noise isn't really noise per-se on the line, but uneven response to tones (and that's what we use in our modems). This can be caused by any number of factors. If you call up good old NONEX and tell them that you have "line noise" your asking for a service bill and no remedy. You will find that the average lineman they send out, has the IQ of his shoe size. Case in point-the old number I used to run my bbs at. I had phantom rings on the line, so did my neighbor across the street. When it was very damp or had rained for a while (several days) the "line noise" would appear, and cause me grief. Well,with the similar problem and a moisture related one at that across the street, it seems like the problem is out around the pole in front of my place. Well,after three visits, and three phantom excuses for repairing it needless to say I was pissed.(The CO will often blast the phone line with what it calls cable test voltage. Its around 600 volts and will vaporize the MOV surge protector in your modem or answering machine) MOV= Metal Oxide Varistor for you non-techies. But it will clear many of their "bad lines". Now one fine day, they finally send out a guy from the "Cable department" and I talk to him, I explain the past problems and suggest he check past my place and for some reason during wet times, we have inter-cable leakage. He found a spot down the street that had been zapped by lightning some time before, and all the wire ends were charred and black. He showed me a ball of burnt wire that could very well been the cause. Well it was, as the problem is lessened about 95%. I say 95% because I still have a bit of the same problem, possibly due to another charred spot or a more recent lightning strike. But this problem seems to respond to my calling my number and letting it ring for say a half hour, this drys out the line enough that it stops acting screwy. Well on to the noises that can be heard over the line that really do have influence over transmission quality. The most prevalent is a crackling or a dial tone drawn intermittently. (Listen to the line with a hi-z butset) Ringing voltage is usually about 90 volts and20-30 hz, so there's usually no problem in ringing the phone, but when you pick up, the phone voltage drops to 30-50 volts and the smallest problem will surface. The phone company has this habit of checking the line to ground (it should never be connected in a regular home phone line) and they will clear off water, insects, and other crap with a 600 volt blast as mentioned earlier. This applied across the line to ground sure does away with the water, but in caes where spike protection or impulse protection from lightning is present, WATCH OUT! the MOV's are typically manufactured to short at around 130-150 volts, and are connected to the third pin (Ground) of a three wire plug on your answering machine, your cordless phone, and some modems. The MOV will explode as it shorts itself to ground to do its job of surge protection, leaving a short on the line which is readily detectable by the CO. IF THIS HAPPENS, inform

them immediately that you have a problem, and they will make restitution for repairs in CASH! I got $75 for repairing a $1.98 MOV (available at Radio Slack)

Now more on the noises....

After the infamous popping, the next most bothersome to the modemer is a low level whine, muchlike some of the shitty MCI ports,sounding like a jet engine varying in rpm, it is particularly evident behind

dialtone, and if you drop the dialtone, its still evident. This is digital whine caused by some circuit in the path not exactly in phase. This is particularly annoying because the digital equipment tries to compensate by stuffing or removing bits from the digital path to attempt

phase lock, and thus, data is occasionally lost or garbled. I have two lines at home that are heavily used and have this problem, its not apparent to modem traffic until you hit 2400 baud, then the time frame of the modem kinda gets jitters from the digital whine. Lastly, of importance, is signal level. In analog, as the signal goes down, the signal tends to corrupt on the lowest levels while some will pass fine during peaks. If this is the problem, you see multiple errors on x-modem, then good blocks.. this problem can have numerous causes, fading of a microwave path, followed by a switching of diversity receivers, bringing the signal backup to par temporarily. Also in this category are bad amps at either the CO or in your own equipment, that won't limit gain till noise actually takes the place of the signal, This is a "slow attack" increase of noise followed by a quick quieting as the redundant amp takes over (In your CO).

Crosstalk:

If you have ever picked up the phone and swore you could hear someone else talking or in some cases, actually been able to talk to the other party, you have been exposed to crosstalk. This obviously will knock the shit outa a modem conversation due to the fact the voice is mixing non-linearly with the data or in some cases, overpowering the data signal itself. This is a fairly common problem, common to analog FDM multiplex equipment. This equipment tries to keep the conversations apart using SSB channels arranged throughout a radio's baseband (IF) frequency. Because the channels are without carrier which would enable the equipment to check signal level, frequencies called "pilots" are inserted into the clusters of channels allowing their levels to be monitored and controlled.If there is a "Hot" pilot or a "Hot" channel in the group, it will bleed over into the other channel's passband and crosstalk will be heard. In the cases of two-way communications via crosstalk, the group pilot is usually so hot, everybody in both directions is splashing over and both directions are being heard. Basically the solution to line noise problems is to know about them, and being able to pinpoint the exact type of problem will make it easier for the Telco to service it quickly.